1. Személyi számítógépek felépítése

1.1 Személyi számítógépek és alkalmazások

1.1.1 Hol és hogyan használjuk a számítógépeket?

A számítógépek egyre fontosabb és csaknem nélkülözhetetlen szerepet játszanak mindennapjainkban.

Számítógépeket különböző felhasználási területeken használnak szerte a világon. Használják őket az üzleti életben, gyártási környezetekben, otthon, kormányzati irodákban és non-profit szervezeteknél. Az iskolákban a számítógépeket a tanításhoz és a diákok adatainak nyilvántartásához használják. A kórházakban a számítógépeket a betegek adatainak nyilvántartására és az orvosi ellátás biztosításához használják.

Ezeken a számítógépeken kívül számos speciális célra tervezett számítógép is létezik. Az ilyen egyedi igényeket kielégítő számítógépek olyan eszközökbe integrálhatók, mint a televízió, pénztárgép, hangrendszerek vagy más elektronikus készülékek. Sőt olyan készülékekben is megtalálhatók, mint a tűzhely vagy a hűtőszekrény, valamint autókban és repülőgépekben is használják őket.

Számítógépeket különböző céllal a legváltozatosabb helyeken használnak. Különböző méretűek és teljesítményűek lehetnek, de vannak közös tulajdonságaik. A megfelelő működés érdekében három dolognak minden számítógépben együtt kell működnie:

1. **Hardver** - mind külső, mind belső fizikai összetevők, a számítógép alkotóelemei.
2. **Operációs rendszer** - olyan programok halmaza, mely kezeli a számítógépes hardvert. Az operációs rendszer szabályozza az erőforrások használatát, beleértve a memóriát és a lemezes tárolót is. Operációs rendszerre példa a Windows XP.
3. **Alkalmazás** - számítógépre telepített program, mely a számítógép adottságait kihasználva speciális feladatokat lát el. Alkalmazásra példa a szövegszerkesztő program, valamint a számítógépes játék.

1.1.2 Helyi és hálózati alkalmazások

A számítógép használhatósága a rajta futó programoktól és alkalmazásoktól függ. Az alkalmazások két általános kategóriába sorolhatók:

Üzleti/Ipari szoftver - speciális ipari vagy üzleti használatra tervezett szoftver. Példák: egészségügyi programok, oktatási programok, jogi szoftverek.

Általános célú szoftver - Szervezetek széles körében vagy otthoni környezetben, különböző célokra használható szoftver. Ezeket az alkalmazásokat bármely cég vagy egyén használhatja.

Általános célú szoftverekhez tartoznak az olyan integrált alkalmazás csomagok, mint az Office csomag. Az ilyen csomagok leggyakoribb összetevői a szövegszerkesztő, a táblázatkezelő, az adatbázis-kezelő, a bemutató-készítő valamint az elektronikus levelező, kapcsolat- és naptárkezelő program.



További népszerű alkalmazások a képszerkesztő és multimédia anyag készítő programok. Ezekkel az eszközökkel lehet képeket szerkeszteni, és gazdag multimédiás bemutatókat készíteni, melyek hangot, videót és grafikát egyaránt tartalmazhatnak.

A szoftverek ipari/üzleti vagy általános célú csoportosítása mellett az alkalmazások a helyi vagy hálózati kategóriákba is besorolhatóak.

Helyi alkalmazás - A helyi alkalmazás olyan program (pl.: szövegszerkesztő), mely a számítógép merevlemezén található. Az ilyen alkalmazás csak az adott számítógépen fut.

Hálózati alkalmazás - A hálózati alkalmazást arra tervezték, hogy hálózaton (pl. az Interneten) keresztül működjön. Egy hálózati alkalmazásnak két összetevője van, az egyik a helyi, a másik egy távoli számítógépen fut. Hálózati alkalmazásra példa az elektronikus levelezés.

A legtöbb számítógépen helyi és hálózati alkalmazások is futnak.

1.2 Számítógépek típusai

1.2.1 Számítógépek osztályozása

Számos különböző típusú számítógép létezik, mint például:

- Nagyszámítógépek
- Kiszolgálók
- Asztali számítógépek
- Munkaállomások
- Laptopok
- Kézi hordozható eszközök

Mindegyik típusú számítógép valamilyen különleges céllal készült, mint például helyváltozás közbeni információ hozzáférés vagy nagyfelbontású képek feldolgozása, stb.

Az otthoni, illetve üzleti életben leggyakrabban használt számítógép típusok a kiszolgálók, munkaállomások, asztali számítógépek, laptopok és más hordozható eszközök. A nagyszámítógépek olyan központi nagygépek, melyeket általában nagyvállalatoknál használnak, és csak erre specializálódott viszonteladóknál szerezhetők be.

1.2.2 Kiszolgálók, asztali számítógépek és munkaállomások

Kiszolgálók

A kiszolgálók nagyteljesítményű számítógépek, melyeket vállalatoknál és más szervezeteknél használnak. A kiszolgálók sok végfelhasználó vagy ügyfél számára nyújtanak szolgáltatásokat.

A kiszolgálók hardverfelépítését egyidejűleg több hálózati kérésre adott kis válaszidőre optimalizálták. A kiszolgálók több Központi Feldolgozó Egységgel (CPU), nagy véletlen hozzáférésű memóriával (RAM) és több nagy kapacitású merevlemezes meghajtóval rendelkeznek, melyek gyors információ hozzáférést biztosítanak.



A kiszolgálók által nyújtott szolgáltatások gyakran igen fontosak, és állandó rendelkezésre állást igényelnek. Ezért a kiszolgálók a kiesés megelőzésére gyakran tartalmaznak duplikált vagy redundáns elemeket. Automatikus és manuális biztonsági mentést is rendszeres időközönként végeznek. A kiszolgálókat általában biztonságos, ellenőrzött hozzáférésű helyen tárolják.

Kivitelezésük eltérő lehet: lehetnek önálló torony kialakításúak, állványra szerelhetők vagy blade (penge) rendszerűek. Mivel a kiszolgálókat általában tárolóegységként, nem napi használatú végfelhasználói berendezésként alkalmazzák, így nem szükséges, hogy saját monitorral vagy billentyűzettel rendelkezzenek, elég, ha ezeket más eszközökkel megosztják.

A kiszolgálók által leggyakrabban nyújtott szolgáltatások a fájltárolás, elektronikus levelek és web oldalak tárolása, nyomtatás megosztás és mások.

Asztali számítógépek

Az asztali számítógépek különböző adottságokkal bírnak. Gépházak, tápegységek, merevlemezek, videokártyák, monitorok és más összetevők széles választéka létezik. Az asztali számítógépek több különböző csatlakozóval és videó kimenettel rendelkezhetnek, valamint perifériák széles választékát támogatják.

Az asztali számítógépeket általában szövegszerkesztő, táblázatkezelő és hálózati alkalmazások, mint például elektronikus levelezés, web böngészés futtatására használják.

Létezik egy másik fajta számítógép is, mely hasonló az asztali számítógéphez, de sokkal nagyobb teljesítményű: a munkaállomás.

Munkaállomás

A munkaállomások nagyteljesítményű vállalati számítógépek. Specializált, magas színvonalú alkalmazásokra tervezték, mint például a CAD (Computer Aided Design - számítógéppel támogatott tervezés) mérnöki program. Munkaállomásokat használnak 3D grafikák, video animációk valamint virtuális valóság szimulációk készítése során. Távközlési vagy egészségügyi berendezések felügyeletére szintén használhatók a munkaállomások. Hasonlóan a kiszolgálókhoz, a munkaállomások jellemzően több CPU-t, nagy mennyiségű RAM-ot és több nagy kapacitású, gyors hozzáférésű merevlemezt tartalmaznak. Munkaállomások általában kiemelkedő grafikai teljesítménnyel és nagy vagy több monitorral rendelkeznek.

A kiszolgálók, asztali számítógépek és munkaállomások mind helyhez kötött eszközök. A laptopokkal ellentétben nem hordozhatóak.

1.2.3 Hordozható eszközök

A helyhez kötött számítógépek mellett számos hordozható elektronikus eszköz is létezik.

Ezek a hordozható eszközök, mind méretben, mind teljesítményben, valamint grafikai képességükben különböznek, és ide tartoznak:

- Laptop vagy notebook PC
- Tablet PC
- Pocket PC
- Digitális személyi asszisztens PDA



- Játékeszköz
- Mobiltelefonok

A laptopok, vagy más néven notebookok használhatóságukban és teljesítményükben hasonlóak az asztali számítógépekhez. Azonban kis súlyú és kis energiafelhasználású hordozható eszközök, melyek beépített egérrel, monitorral és billentyűzettel rendelkeznek. A laptopokat csatlakoztathatjuk dokkoló állomáshoz, mely segítségével a felhasználó nagyobb monitort, egeret és teljes méretű billentyűzetet használhat, valamint több kapcsolódási lehetőség közül választhat.

Ennek ellenére a laptopok általában korlátozottabb lehetőséggel rendelkeznek például a megjelenítési képességek és a csatlakozási típusok terén, és a bővítésük sem olyan egyszerű, mint az asztali számítógépek esetén.

Más hordozható eszközök, mint például a PDA-k vagy pocket PC-k, kisebb teljesítményű CPU-val és kevesebb RAM-mal rendelkeznek. Korlátozott kijelző funkcióval ellátott képernyőjük és kis billentyűzetük van.

A hordozható számítógépek legnagyobb előnye, hogy az információ és a szolgáltatások azonnal és szinte bárhonnan elérhetők. Például a mobil telefonok beépített címjegyzékkel rendelkeznek, melyben a kapcsolat neve és telefonszáma tárolható. A PDA-k beépített telefonnal, web böngészővel, elektronikus levelező programmal és más szoftverekkel is kaphatók.

Az egyes eszközök funkciói egyesíthetők egy multifunkcionális eszközben is. A multifunkcionális eszköz egyesíthet egy PDA-t, mobiltelefont, digitális kamerát és egy zene lejátszót. Internet hozzáférést és vezeték nélküli hálózatelérést biztosíthat, de a PDA-khoz hasonlóan korlátozott feldolgozási teljesítménnyel rendelkezik.

1.3 Az adatok bináris ábrázolása

1.3.1 Az információ digitális ábrázolása

A számítógépekben az adatok digitális, bináris formában találhatók. A bit a bináris számjegy (BInary digiT) rövidítése és egyben a legkisebb adategységet reprezentálja. Az emberek szavakat és képeket értelmeznek; a számítógépek csak bitmintákat tudnak feldolgozni.

Egy bit két értéket vehet fel: egyes számjegyet (1) vagy nullás számjegyet (0). Egy bit reprezentálhatja bárminek az állapotát, melynek két állapota létezik. Például a lámpakapcsoló vagy "Kikapcsolt" vagy "Bekapcsolt" állapotban lehet; binárisan ezek az állapotok megfeleltethetők az 1-nek és a 0-nak.

A számítógépek bináris kódokat használnak a betűk, számok és más speciális karakterek bitekkel történő ábrázolására. A leggyakrabban használt kód az ASCII (American Standard Code for Information Interchange). ASCII kódolás esetén minden karakternek egy bitsorozat felel meg. Például:

Nagybetű: A =01000001

Szám: 9 = 00111001

Speciális karakter: # = 00100011

A betűk és számok ábrázolásánál is használt 8 bitből álló csoportot bájtnak nevezzük.

Kódolást lehet használni szinte valamennyi információtípus (számítógépes adat, grafika, kép, hang, videó, zene) digitális formában történő ábrázolására.

1.3.2 Tárolókapacitás mérése

Bár a bit jelöli a legkisebb adategységet, az adattárolás legalapvetőbb egysége mégis a bájt. Egy bájt nyolc bitből áll és egyben a legkisebb mértékegységként használjuk a tárolókapacitás leírására.

Amikor a tároló méretére utalunk, általában a bájt (B), kilobájt (KB), megabájt (MB), gigabájt (GB) és terabájt (TB) mértékegységeket használjuk.

Egy kilobájt egy kicsivel több, mint ezer bájt, pontosan 1024 bájt. Egy megabájt több mint egy millió, pontosan 1,048,576 bájtot jelöl. Egy gigabájt 1,073,741,824 bájt és így tovább. A pontos értékek a kettő megfelelő hatványából adódnak. Példa: KB = 2^10; MB = 2^20; GB = 2^30.

Általánosan elmondható, hogy digitális ábrázolás esetén minél több a részlet annál több bit szükséges az adat reprezentálásához. Egy digitális kamerával felvett alacsony felbontású kép körülbelül 360KB, egy nagy felbontású kép akár 2 MB vagy több is lehet.

Kilobájtokat, megabájtokat, gigabájtokat és terabájtokat tipikusan egy eszköz tárolókapacitásának vagy méretének leírására használjuk. Példa eszközökre és alkotóelemekre melyek bájtokat tárolnak: véletlen hozzáférésű memória (RAM), merevlemezes meghajtó, CD-k, DVD-k és MP3 lejátszók.

1.3.3 A sebesség, felbontás és frekvencia mérése

A digitális információ egyik előnye, hogy nagyobb távolságon is közvetíthető a minőség romlása nélkül. A modem a bináris jelet az átviteli közegen átvihető formára alakítja.

Leggyakrabban használt átviteli közegek:

- Kábelek, melyek elektromos impulzusokat használnak rézvezetékeken
- Üvegszálas optika, mely a fény impulzusait használja üvegből vagy műanyagból készült üvegszálakon
- Vezeték nélküli technológia, mely kis teljesítményű rádióhullámok impulzusait használja

Egy fájl méretének a leírására két mértékegységet használunk: biteket (b) és bájtokat (B). A távközlési mérnökök átvitt bitekben, míg a felhasználók inkább Byte-okban (kilobyte, megabyte) mért fájlméretben gondolkodnak. Egy bájt 8 bitet reprezentál.

Az átviteli sebesség megadja, hogy mennyi időre van szükség egy fájl letöltéséhez. Minél nagyobb egy fájl, annál több idő kell a letöltéséhez. Az átviteli sebesség mértékegysége az ezer bit/másodperc (kbps) vagy millió bit/másodperc (Mbps). Figyeld meg, hogy a kbps rövidítésben kis k betű szerepel nagy K helyett. Ennek az oka, hogy átviteli sebesség esetén gyakran kerekítünk lefelé. Valójában a kbps jelöli 1000 bit információ 1 másodperc alatti letöltését, míg a kbps az 1024 bit/másodperc átviteli sebességre utal. DSL vagy kábelmodem esetében az alkalmazott technológiától függően 512 kbps, 2 mbps vagy nagyobb sebességek érhetők el.

Letöltési idő

A számított letöltési idő egy elvi érték, amely függ a hálózati csatlakozástól, a számítógép processzorának sebességétől és egyéb paraméterektől. Egy fájl letöltéséhez szükséges idő becsléséhez a fájl méretét kell az átviteli sebességgel elosztani. Mennyi ideig tart például egy kis felbontású, 256 KB-os digitális fénykép letöltése egy 512 kbps-os hálózati kapcsolaton? Első lépésként váltsuk át a fájl méretét bitekre: 8 x 256 x 1024 = 2097152 bit. 256 KB-nak 2097 kb felel meg. Figyeld meg, hogy a 2097152-t kerekítettük ezresekre, így kis k betűt használtunk. A letöltési idő így 2097 kb osztva 512 kbps-al, ami hozzávetőleg 4 másodperc.

A tárolókapacitás és átviteli sebesség mellett számítógépek esetében egyéb mértékegységeket is használunk.

Számítógép képernyőjének felbontása

A grafikus felbontást pixelben adják meg. Egy pixel a képernyőn megjelenő egyetlen fénypont. A számítógép képernyőjének minőségét a függőlegesen és vízszintesen megjeleníthető pixelek száma adja meg. Egy szélesvásznú monitor például 1280 x 1024 pixelt és több millió színt képes megjeleníteni. Digitális kamera felbontását az egy képet alkotó megapixelek száma adja.

Analóg frekvenciák

A hertz a periódikus változások illetve frissülések gyorsaságának mértékegysége. 1 hertz másodpercenként egy periódust jelent. Számítógépek esetében a processzor sebességét hertz-ben mérjük, amely megadja a feladatok végrehajtási periódusainak sebességét. Egy 300 MHz-zel működő processzor például 300 millió periódust hajt végre másodpercenként. A vezeték nélküli átvitelt és a rádófrekvenciákat is hertz-ben mérjük.

1.4 A számítógép alkotóelemei és perifériái

1.4.1 Számítógép rendszer

Sokféle számítógép létezik. Mitől válik alkalmasabbá egy számítógép játékok vagy hangfájlok futtatására? A válasz: a számítógép alkatrészeitől és perifériáitól.

Egy elsősorban szövegszerkesztésre használt számítógép követelményei lényegesen eltérnek egy grafikus alkalmazásokat vagy játékokat futtató géphez képest. Mielőtt eldöntjük, milyen típusú és felszereltségű számítógépet vegyünk, fontos meghatároznunk, mire szeretnénk használni.

Sok gyártó sorozatban állít elő olyan számítógép rendszereket, amelyeket közvetlenül vagy kiskereskedelmi láncon keresztül értékesít. Ezeket a számítógépeket úgy tervezték, hogy alkalmasak legyenek több különböző típusú feladat elvégzésére is. Szintén sok forgalmazó kínál a felhasználók igényeit kielégítő, speciálisan összeállított számítógépet. Mindkettőnek megvannak az előnyei és hátrányai.

Előre összeállított számítógép

Előnyök:

- Alacsonyabb költség
- A legtöbb alkalmazás futtatására alkalmas
- Összeszerelése nem igényel időt
- Leginkább különleges igényekkel nem rendelkező, kevésbé képzett felhasználók számára hasznos

Hátrányok:

- Gyakran hiányzik az a teljesítményszint, ami egyéni igények szerint összeállított számítógép esetén elérhető

Egyéni igények szerint összeállított számítógép

Előnyök:

- A felhasználó határozhatja meg, milyen összetevőkre van szüksége
- Általában nagyobb teljesítményt igénylő, mint pl. grafikai, játék és szerveralkalmazásokat támogat

Hátrányok:

- Általában lényegesen költségesebb, mint egy előre összeállított számítógép
- Összerakása időt igényel

A számítógép egyes alkotóelemei külön-külön is beszerezhetők és összerakhatók. Függetlenül attól, hogy milyen típusú rendszer mellett döntöttünk (előre vagy igény szerint összeállított) vagy magunk állítottuk össze, a számítógépnek a felhasználó igényeit kell teljesíteni. Néhány fontos szempont számítógép vásárlásakor: alaplap, processzor, RAM, tároló, illesztőkártyák paraméterei valamint gépház és áramellátási lehetőségek.

1.4.2 Alaplap, CPU és RAM

Az alaplap egy nagy nyomtatott áramkör, amely a számítógépet alkotó elektronikai elemeket és áramköröket köti össze. Az alaplap csatlakozókat tartalmaz, melyek lehetővé teszik a fő rendszerelemek, mint CPU és RAM csatlakoztatását. Az alaplap szállítja az adatokat a különböző csatlakozók és rendszerelemek között.

Az alaplapon lehetnek továbbá olyan csatlakozóaljzatok, amelyekhez hálózati, videó - és hangkártya illeszthető. Azonban ma már egyre több alaplapot úgy fejlesztenek, hogy ezeket a funkciókat integráltan tartalmazzák. A két megoldás közti különbséget a bővíthetőség adja. Csatlakozók használatakor a rendszerelemek könnyedén eltávolíthatók, és a technikai fejlődést követve cserélhetők vagy bővíthetők.

Egy beépített funkció bővítése vagy cseréje során maga a funkció nem távolítható el az alaplapról. Éppen ezért gyakran van szükség egy integrált funkció letiltására és egy csatlakozóba illesztett kártya használatára.

Alaplap választásakor a következőket kell figyelembe venni:

- Támogassa a kiválasztott CPU típusát és sebességét.
- Támogassa az alkalmazásokhoz szükséges rendszer RAM típusát és mennyiségét.
- Megfelelő mennyiségű és típusú bővítőhellyel rendelkezzen az összes szükséges interfészkártya csatlakoztatásához.
- Elegendő és megfelelő típusú interfésszel legyen ellátva.

Központi feldolgozó egység (CPU)

A CPU vagy processzor a számítógép központi idegrendszere. Ez az alkotóelem dolgozza fel az adatokat a számítógépen belül. Számítógép rendszer létrehozásának vagy frissítésének első lépése a CPU típusának kiválasztása. Ennek fontos szempontjai, a processzor és a busz sebessége.

Processzor sebesség

A processzor sebessége az információ feldolgozásának sebessége. Ezt általában MHz-ben vagy GHz-ben mérjük. Minél nagyobb a sebesség, annál nagyobb a teljesítmény. Egy gyorsabb processzor több energiát fogyaszt, és több hőt termel. Éppen ezért a mobil eszközök, mint pl. egy laptop, lassabb processzort és így kevesebb energiát használnak annak érdekében, hogy minél hosszabb ideig működjenek akkumulátor használatával.

Busz sebesség

A CPU az alaplapon található különböző típusú memóriák között irányítja az adatokat. Az adatok ilyen áramlásának útját hívjuk busznak. Általában minél gyorsabb a busz, annál gyorsabb a számítógép is.

A CPU kiválasztásakor vegyük figyelembe az alkalmazások folyamatos fejlődését. Egy átlagos sebességű CPU vásárlásával a pillanatnyi követelményeket elégíthetjük ki. A jövőben viszont bonyolultabb, például nagy felbontást igénylő alkalmazásoknál, egy nem megfelelő sebességű CPU a számítógép egész teljesítményét lerontja, ami a válaszidő megnövekedésével jár.

A CPU az alaplap egyik csatlakozójába illeszkedik és általában az alaplaphoz csatlakozó legnagyobb méretű alkatrész. Az alaplapnak a kiválasztott processzorral kompatibilis csatlakozóval kell rendelkeznie.

RAM

A RAM a számítógépeknél használt adattárolók egy típusa. A RAM-ot a CPU által feldolgozás alatt lévő programok és adatok tárolására használják. A adatok elérése történhet a tárolási sorrendnek megfelelően vagy véletlenszerűen is. Minden számítógépes program a RAM-ból fut. A CPU után a RAM mennyisége befolyásolja leginkább a számítógép teljesítményét.

Minden operációs rendszer igényel a futtatásához egy minimális mennyiségű RAM-ot. A legtöbb számítógép képes egyszerre több alkalmazás futtatására, illetve több feladat egyidejű elvégzésére. Sok felhasználó egyidejűleg használ például levelező programot, azonnali üzenetküldő alkalmazást, vírus elleni eszközöket vagy tűzfalat. Ezek az alkalmazások mind memóriát igényelnek. Minél több a párhuzamosan futó program, annál több memóriára van szükség.



A többprocesszoros számítógéprendszerek is nagyobb memóriaigénnyel rendelkeznek. Ezenfelül a CPU és a busz sebességének növekedését a memória sebességének is követnie kell. A számítógépbe telepíthető RAM típusát és mennyiségét az alaplap határozza meg.

1.4.3 Illesztőkártyák

Az illesztőkártyák a számítógép szélesebb körű felhasználási lehetőségét biztosítják. Tervezésüknek köszönhetően a számítógép alaplapjának csatlakozójába vagy aljzatába illesztve a rendszer részévé válnak. Sok alaplap úgy van tervezve, hogy ezeknek az illesztőkártyáknak a feladatát integráltan magában foglalja, így nincs szükség az egyes kártyák beszerzésére és telepítésére. Míg ezek az alaplapok az alapvető funkciókat látják el, addig egyedi kártyák használatával nagyobb teljesítményszint érhető el.

Néhány gyakran használt illesztőkártya:

- Videokártyák
- Hangkártyák
- Hálózati kártyák
- Modemek
- Interfészkártyák
- Vezérlőkártyák

1.4 4 Tárolóeszközök

A tápellátás megszűnésével a RAM tartalma elvész. A programokat és felhasználói adatokat olyan helyen kell tárolni, ahol akkor sem vesznek el, ha a tápellátás megszűnik. Ezt hívjuk nem felejtő tárolónak. Különböző típusú nem felejtő tárolók léteznek, úgy mint:

- Mágneses tároló eszközök
- Optikai tároló eszközök
- Statikus memória (flash) meghajtók

Mágneses tároló

A mágneses tárolók az adatok tárolására leggyakrabban használt eszközök. Ezek az eszközök mágneses mező segítségével tárolják az információt. Ilyenek például:

- Merevlemez meghajtók
- Hajlékonylemez meghajtók
- Szalagos meghajtók

Optikai meghajtók

Az optikai tároló eszközök lézersugár segítségével az optikai sűrűség változtatásával rögzítik az információt. Ilyen eszközök a CD-k és DVD-k, melyeknek három típusát különböztetjük meg:

- Csak olvasható: CD, DVD
- Egyszer írható:CD-R, DVD-R
- Többször írható: CD-RW, DVD-RW

Ezeknek az eszközöknek az ára folyamatosan csökken, és ma már a legtöbb számítógép DVD-RW meghajtóval kapható, melyhez tartozó egyoldalas lemez kapacitása 4.7 GB.

A DVD meghajtók egy másik formája az úgynevezett Blu-ray. Az adatok olvasásához és írásához másfajta lézert használ. Az információ tároláshoz használt lézer színe ibolyakék. Ennek köszönhetően hívják Blu-ray lemeznek, megkülönböztetve így a hagyományos DVD-től, mely piros lézerfényt használ. A Blu-ray lemezek tárolókapacitása 25 GB vagy annál nagyobb.

Statikus memória és memória modulok

A statikus memória eszközök memóriachipen tárolják az információt. Az itt tárolt információk a gép kikapcsolása után is megmaradnak. A számítógép egy USB portjához csatlakoznak és 128 vagy még több MB tárolására képesek. Méretükből és alakjukból adódóan ezek az eszközök USB memória vagy Flash memóriaként ismertek és fájlok hordozásánál széleskörűen helyettesítik a floppy lemezeket. Sok hordozható eszköz és kézi készülék adattárolásra teljes egészében statikus memóriát használ.

Tároló kapacitás vásárlásakor általánosan elfogadott gyakorlat a mágneses és az optikai memóriák keverése, akár statikus memóriával is. Amikor a tárolókapcitás nagyságáról döntünk, a becsült igényhez képest további 20%-os többlettel kell számolni a későbbi igények miatt.

1.4.5 Perifériák

A periféria egy számítógéphez csatlakoztatott eszköz, mely kiterjeszti annak képességeit. Mivel ezek az eszközök nem szükségesek az alapfunkciók ellátásához, ezért alkalmazásuk nem kötelező, ugyanakkor jelentősen növelhetik a számítógép használhatóságát. A perifériák kívülről csatlakoznak a számítógéphez, speciális kábelt vagy vezeték nélküli technológiát használva.

A perifériák négy csoportba sorolhatók: bemeneti, kimeneti, tároló és hálózati eszközök. Közismert perifériák a következők:

- **Bemeneti eszközök:** trackball, botkormány, lapolvasó, digitális fényképezőgép, digitalizáló, vonalkód olvasó, mikrofon
- **Kimeneti eszközök:** nyomtató, rajzgép, hangszórók, fejhallgatók
- **Tároló eszközök:** másodlagos tároló, külső CD/DVD készülékek, flash memóriák
- **Hálózati eszközök:** külső modemek, külső hálózati kártya (NIC)

1.4.6 Számítógépházak és tápegységek

A számítógépház és tápegység

A belső tartozékok és a csatlakozók után a számítógépház a következő összetevő amit megvizsgálunk. A számítógépházak egy részét az asztal tetején, míg másik részét az asztal alatt történő elhelyezésre tervezik. Az asztalra tervezett számítógépek könnyű hozzáférést biztosítanak az interfészekhez és meghajtókhoz, azonban értékes asztalterületet igényelnek. A torony és mini torony házak elhelyezhetők az asztal alatt és fölött egyaránt. Típustól függetlenül a számítógépház kiválasztásánál az a legfontosabb szempont, hogy elegendő helyet biztosítsanak a beépítendő komponensek számára.

A számítógépház és a tápegység általában együtt kapható. A tápegységnek elegendő teljesítményűnek kell lennie, hogy mind a rendszert, mind az esetlegesen később csatlakoztatott eszközöket elegendő elektromos energiával lássa el.

A számítógép folyamatos áramellátást igényel. Az áramszolgáltatók által biztosított elektromos áramellátásban feszültségcsökkenés vagy áramkimaradás is jelentkezhet. A rossz áramellátás befolyásolhatja a számítógép hardverelemeinek teljesítményét, és a károsodásukat is okozhatja. További következményként a számítógépen tárolt szoftverek és adatok is megsérülhetnek.

A számítógépet az áramellátással kapcsolatos problémákkal szemben többféle eszközzel is védhetjük. Ilyen készülék például a túlfeszültségvédő és a szünetmentes tápegység (uninterruptible power supplies, USP).

Túlfeszültségvédő

A túlfeszültségvédők a feszültségtüskéket és a túlfeszültséget elvezetik az elektromos vezetékről, ezzel megelőzve a gép károsodását. Viszonylag olcsók, és könnyen üzembehelyezhetők.

Általában a túlfeszültségvédőt az elektromos fali aljzatba, a számítógépet pedig a túlfeszültségvédőbe kell csatlakoztatni. Számos túlfeszültségvédőhöz telefonvezeték is csatlakoztatható, hogy megvédje a modemet a telefonvonalon érkező túlfeszültségtől.

Szünetmentes tápegység

Az UPS olyan eszköz, melyben egy beépített akkumulátor segítségével a rendszer áramellátása folyamatosan nyomon követhető és fenntartható. Ha az áramellátás megszakad, az UPS szolgál tartalék árammal a számítógép szünetmentes működéséhez. A tartalék áramot a UPS-ben elhelyezett akkumulátor adja, és csak rövid ideig használható. Az UPS-t úgy tervezték, hogy a felhasználónak elegendő ideje legyen a számítógép megfelelő kikapcsolásához áramszünet esetén. Az UPS további előnye, hogy egyenletes áramellátást biztosít, és megelőzi a túlfeszültség okozta károkat.

Az otthonok és kisebb vállalatok számára tervezett UPS-ek viszonylag olcsók, emellett gyakran magukba foglalják a túlfeszültségvédőt és az áramellátás stabilitását biztosító egyéb eszközöket. A számítógépek UPS-el való védelme erősen ajánlott a gép helyétől és felhasználási területétől függetlenül.

1.5 A számítógépes rendszer összetevői

1.5.1 Biztonsági előírások és gyakorlati tanácsok

A számítógép bonyolult alkatrészek és perifériák együttese, amelyek közös munkával látnak el bizonyos feladatokat. Meghibásodás miatt, vagy a rendszer teljesítőképességének növelése érdekében egyes alkatrészek időnként cserére szorulhatnak. Ehhez gyakran a számítógépház felnyitására, és a házon belül történő szerelésre van szükség.

Az ilyen munka során fontos a biztonsági óvintézkedések betartása, hogy megelőzzük a rendszer komponenseinek rongálódását, vagy a szakember sérülését. Mielőtt a gépházat felnyitjuk, győződjünk meg róla, hogy a számítógépet kikapcsoltuk és áramtalanítottuk!

A számítógép és a monitor szállítását esetlegesen nagy súlyuk miatt óvatosan kell végezni! A számítógép felnyitása előtt biztosítani kell a megfelelő munkaterületet. A munkaterület legyen tiszta és sík felület, és elég erős ahhoz, hogy elbírja a súlyosabb berendezéseket. Legyen zsúfoltságtól és rendetlenségtől mentes, valamint a szem megerőltetésének elkerülése végett jól megvilágított!

A szemet megfelelően kell védeni a szennyeződésektől, kisebb csavaroktól és az egyéb alkatrészektől, melyek sérülést okozhatnak. A gépház felnyitásánál az éles peremek érintését el kell kerülni!

A tápegységek és képernyők veszélyesen magas feszültséggel működnek, ezért kizárólag képzett szakemberek nyithatják fel.

Egyes számítógépek esetén a komponenseket üzem közbeni cserére is alkalmassá tették, ami a gép kikapcsolása nélkül teszi lehetővé az összetevők csatlakoztatását, illetve eltávolítását. (Angolul az ilyen alkatrészeket hot-swappable eszközöknek, magát a technológiát hot-swapping-nek nevezik.) Ennek a tulajdonságnak köszönhetően a gép működés közben szerelhető és fejleszthető. A technológiát elsősorban nagyteljesítményű kiszolgálóknál alkalmazzák.

Hacsak nem biztos benne, hogy a rendszer „hot-swappable" mindig kapcsolja ki a gépet, mielőtt felnyitná a számítógépházat, vagy eltávolítana egy alkatrészt! Egy „hot-swapping" tulajdonsággal nem rendelkező számítógép működés közben történő szerelése komoly és maradandó sérülést okozhat a rendszernek vagy a szerelést végző szakembernek.

A belső rendszerkomponensek különösen érzékenyek a statikus elektromossággal szemben. Az elektrosztatikus kisülés (Electrostatic Discharge) ESD statikus elektromosság, ami a testről a gép elektromos alkatrészeire tevődhet át. A statikus elektromosság nem feltétlenül érezhető.

Az ESD végzetes hibákat okozhat az alkatrészekben, működésképtelenné téve azokat. Az ESD következtében kontakthiba is keletkezhet, aminek felderítése meglehetősen nehéz. A felsorolt okokból kifolyólag a megfelelő földelés elsődleges követelmény. A szakemberek egy speciális földelő csuklópántot használnak, hogy testük és a számítógép háza között összeköttetést létesítsenek. A földelés biztosítja a szakember és a rendszer azonos feszültségszintjét, megelőzve ezzel az ESD-t.

Sosem szabad túlzott erővel beszerelni egy komponenst! A túlzott erőltetés megsértheti az alaplapot és a beszerelendő összetevőket is, aminek következtében a rendszer nem fog megfelelően működni. A károsodás nem mindig látható. Az erőltetés a csatlakozóban is kárt tehet, ami később a hozzá csatlakoztatott új komponenseket is tönkreteheti.

Annak érdekében, hogy bizonyosak lehessünk az összes előírás betartásában, ajánlott egy ellenőrző lista készítése, aminek alapján a munkafolyamat elvégezhető.

- Használj antisztatikus alátétet és földelő csuklópántot.
- A számítógép összetevőinek tárolására és mozgatására használj antisztatikus tasakokat. A tasakba egynél több összetevőt ne tegyél, mivel azok feltornyozása egyes összetevők törését vagy kilazulását okozhatja.
- A gép bekapcsolt állapotában ne helyezz a számítógépbe összetevőt vagy ne távolítsd el onnan.
- Gyakran földeld magad a ház vagy tápegység csupasz fémdarabjának megérintésével. Ez megakadályozza a sztatikus feltöltődést.

- Csupasz aljzaton állva dolgozzál, mivel a szőnyegborítás sztatikusan feltöltődhet
- A kártyákat az élüknél fogd meg kerülve a mikrochipek vagy a bővítőkártya csatlakozóélének a megérintését.
- Ne érintsd meg a mikrochipeket vagy a bővítőkártyákat mágneses végű csavarhúzóval.
- Kapcsold ki a számítógépet annak mozgatása előtt. Ez a merevlemez védelmét szolgálja, mely a számítógép bekapcsolt állapotában mindig forog.
- A telepítő/karbantartó CD-ket, lemezeket óvd a mágneses erőtértől, hősugárzástól és a hideg hőmérséklettől.
- Semmilyen áramköri lapot ne helyezz vezető felületre, különösen fémfóliára. Az alaplapon használt lítium és nikkel-kadmium (Ni-Cad) elemekben rövidzár keletkezhet.
- A kétlábsoros (DIP) kapcsolók átváltásához ne használj ceruzát vagy fém végű eszközt illetve ne érintsd meg velük az összetevőket. A ceruzában található grafit vezető, így könnyen károsodást okozhat.
- Ne hagyd hogy bárki, aki nem megfelelően földelt, a számítógép összetevőit megérintse vagy kézzel eltávolítsa azokat. Ez érvényes a laboratóriumban veled együtt dolgozó társadra is. Az öszetevők továbbadásakor az átvevő kezét mindig érintsd meg először az esetleges töltés semlegesítése céljából.

1.5.2 Az összetevők beszerelése és működésük ellenőrzése

A legtöbb összetevőnél az alábbi lépéseket kell elvégezni:

1. Vizsgálja meg, vajon a gép képes-e "hot-swappable” szerelésre? Ha ez nem biztos, a gépház felnyitása előtt a gépet áramtalanítani kell!

2. A földelő csuklópánttal kösse össze a testét a gép keretével vagy vázával, így megelőzhetőek az olyan károsodások, melyeket ESD okoz.

3. Ha kicserél egy alkatrészt, távolítsa el a régit. Az alkatrészek gyakran a vázhoz vannak rögzítve kisméretű csavarokkal vagy csiptetőkkel. Amikor a csavarokat eltávolítjuk, ne engedjük azokat az alaplapra esni! Figyeljünk arra is, hogy ne törjük le a műanyag csiptetőket.

4. Ellenőrizze az új komponens csatlakozójának típusát. Minden kártyát csak a megfelelő típusú csatlakozóval lehet a rendszerbe illeszteni, és nem szabad sem a beillesztésnél, sem a kivételnél erőltetni.

5. Helyezze az új alkatrészt a megfelelő helyre a megfelelő irányban és gondosan végezze el az üzembe helyezéssel járó utasításokat.

Kövesse a biztonsági előírásokat lépésről lépésre.

Az új vagy csereként szolgáló alkatrész beépítése után zárja le a gépházat, és csatlakoztassa újra a táp- és egyéb kábeleket. Kapcsolja be a rendszert, és figyelmesen olvassa el a képernyőn esetlegesen megjelenő üzeneteket! Ha a rendszer nem indul, ismét húzza ki a kábeleket, és ellenőrizze, hogy az alkatrész megfelelően van-e csatlakoztatva! Ha a rendszer továbbra sem indul az új összetevővel, távolítsa el, és próbálja elindítani a számítógépet. Ha az új összetevő nélkül elindul a rendszer, előfordulhat, hogy a komponens nem kompatibilis az aktuális hardverrel vagy szoftverrel és a probléma alaposabb vizsgálatot igényel.



Bizonyos alkatrészek működéséhez további speciális szoftverre vagy illesztőprogramra is szükség lehet. A leggyakrabban használt összetevők illesztőprogramját általában az operációs rendszer tartalmazza, de más speciális komponensek esetében az illesztőprogramot külön kell hozzáadni. Az újabb operációs rendszerek általában figyelmeztetnek, ha további illesztőprogram hozzáadására van szükség.

Az illesztőprogramokat folyamatosan fejlesztik a hatékonyság és a használhatóság növelése érdekében. A legfrissebb illesztőprogram elérhető a gyártó cég honlapjáról és normális esetben ezt kell használni. Az illesztőprogramhoz mellékelt dokumentációt a lehetséges problémákról és a megfelelő üzembe helyezésről minden esetben végig kell olvasni!

Telepítés után a tesztelni kell az alkatrész teljes funkcionalitását.

Az alkatrészeket úgy tervezték, hogy a rendszererőforrások egy meghatározott részét használják. Ha két komponens egyszerre próbálja használni ugyanazt az erőforrást, egyik vagy mindkettő működésképtelenné válhat. Megoldást nyújthat az egyik eszköz által használt erőforrás cseréje. Az újabb alkatrészek és operációs rendszerek dinamikusan foglalják le a rendszer erőforrásait.

Ha az eszköz nem működik megfelelően, ellenőrizni kell, hogy a megfelelő és a legújabb illesztőprogramot használjuk-e. Szintén meg kell vizsgálni, hogy az operációs rendszer felismerte-e, és helyesen azonosította-e az eszközt. Ha a probléma továbbra is fennáll, ki kell kapcsolni a rendszert, ki kell venni, és körültekintően újra behelyezni a komponenst, majd ellenőrizni a csatlakozásokat. A megfelelő beállítások érdekében az eszköz leírását is át kell olvasni. Ha az eszköz továbbra sem működik, előfordulhat, hogy az eszköz gyári hibás, és vissza kell vinni az eladóhoz.

1.5.3 Perifériák beszerelése és működésük ellenőrzése

Ellentétben a belső komponensekkel, a perifériák beszerelése nem igényli a számítógépház felnyitását. A perifériák vezetékes vagy vezeték nélküli kapcsolattal csatlakoznak a rendszerhez, a számítógépház külsején található interfészeken keresztül. A hagyományos perifériákat egy meghatározott típusú csatlakozón keresztül lehetett a rendszerhez kapcsolni. A személyi számítógépek nyomtatóinál például az adat a párhuzamos porton keresztül jutott a gépről a nyomtatóra.

A közelmúltban kifejlesztett univerzális soros busz (Universal Serial Bus, USB) csatlakozó lényegesen egyszerűsíti a kábellel működő perifériás eszközök csatlakoztatását. Az USB eszközök nem igényelnek bonyolult konfigurálást, csupán csatlakoztatni kell őket a megfelelő interfészhez, feltételezve, hogy a megfelelő illesztőprogram telepítve van. Tovább növekszik azon perifériák száma, melyek vezeték nélküli technológia segítségével csatlakoznak az állomáshoz.

Egy periféria üzembe helyezése több lépésben történik. Ezen lépések sorrendje és mikéntje a fizikai kapcsolattól és az eszköz Plug-and-Play (PnP) képességétől függ. A lépések a következők:

- Csatlakoztassa a perifériát az állomáshoz a megfelelő kábellel vagy vezeték nélküli technológiával!
- Csatlakoztassa a perifériát az áramforráshoz!
- Telepítse a megfelelő illesztőprogramot!



Némely régebbi, hagyományos (legacy) eszközként emlegetett periféria nem PnP-képes, ezért ezeknél a csatlakoztatás és bekapcsolás után telepíteni kell az illesztőprogramot.

A PnP USB eszközök esetén az illesztőprogramokat az operációs rendszer előtelepített formában tartalmazza. Ebben az esetben a PnP eszköz csatlakoztatása és bekapcsolása után, az operációs rendszer felismeri az eszközt, és telepíti a megfelelő illesztőprogramot.

Elavult vagy rossz illesztőprogram telepítése előre nem látható hibákhoz vezethet, ezért mindig az elérhető legfrissebb illesztőprogramot kell telepíteni.

Ha a periféria a csatlakoztatás és telepítés után nem működik, ellenőrizni kell a kábeleket és azt, hogy az eszköz be van-e kapcsolva.

Számos eszköz (például a nyomtatók jelentős része) számítógépes kapcsolatot nem igénylő öntesztelési funkcióval rendelkezik. Ezzel a lehetőséggel ellenőrizhető, hogy az eszköz megfelelően működik-e magában. Ha az önteszt hibátlanul lefut, akkor a hiba a kábeles kapcsolatban lehet.

A gyanús kábelt ki kell cserélni egy jó kábelre! Ha a probléma továbbra is fennáll, a következő lépésben ellenőrizni kell, vajon az operációs rendszer felismerte-e az eszköz által használni kívánt portot.

Ha látszólag minden megfelelően működik, előfordulhat, hogy az eszköz nem kompatibilis a jelenlegi hardverrel vagy operációs rendszerrel, és a probléma megoldása további lépéseket igényel.

Miután végeztünk a telepítéssel, a periféria teljes funkcionalitását tesztelni kell. Részleges működés esetén, leggyakrabban az elavult vezérlőprogram okozza a problémát. Ez könnyen orvosolható, ha a gyártó cég honlapjáról letöltjük és telepítjük a legfrissebb verziót.

2. Operációs rendszerek

2.1 Az operációs rendszer kiválasztása

2.1.1 Az operációs rendszer feladatai

A számítógép alkatrészei és a perifériák önmagukban nem jelentenek többet elektronikus és mechanikus elemek gyűjteményénél. Ahhoz, hogy ezek az elemek egymással együttműködve végrehajtsanak egy adott feladatot, speciális számítógépes programra, egy ún operációs rendszerre (OS) van szükség.

Tételezzük fel, hogy egy felhasználó jelentést szeretne írni, majd kinyomtatni azt egy csatlakoztatott nyomtatón. A feladat elvégzéséhez szükség van egy szövegszerkesztőre. Az információ bevitele a billentyűzetről történik, a képernyőn jelenik meg, mentése a merevlemezre történik, végül a nyomtatóra lesz küldve.

A szövegszerkesztőnek ezen feladatok megvalósításához együtt kell működnie a beviteli és kiviteli feladatokat irányító operációs rendszerrel. Ezen felül a bevitt adatok tárolása a RAM-ban történik, feldolgozásukat a CPU végzi. Ezt a folyamatot szintén az operációs rendszer vezérli. Minden számítógép-vezérelt eszköz (pl.: kiszolgálók, asztali gépek, laptopok vagy hordozható eszközök) számára a megfelelő működéshez szükséges egy operációs rendszer.

Az operációs rendszer egyfajta tolmácsként funkcionál a felhasználói alkalmazások és a hardver között. A felhasználói alkalmazásokon (pl.: szövegszerkesztőn, táblázatkezelőn, számítógépes játékon vagy azonnali üzenetküldő programon) keresztül kommunikál a számítógép-rendszerrel. Az alkalmazásokat adott feladatokra tervezik, mint például szövegszerkesztésre, és nincs tudomásuk a háttérben működő elektronikáról. Az alkalmazás szempontjából például egyáltalán nem lényeges, hogy az információ miként jut a billentyűzetről az alkalmazáshoz. Az operációs rendszer felel az alkalmazás és a hardver közötti kommunikációért.

A számítógép bekapcsolása után történik az operációs rendszer betöltése, általában valamely lemezmeghajtóról a RAM-ba. Az operációs rendszer kódjának a számítógépes hardverrel közvetlenül kommunikáló része a rendszermag (kernel). Az operációs rendszert az alkalmazásokkal és a felhasználóval összekapcsoló része a parancsértelmező. A felhasználó a parancssoros kezelőfelületen (CLI: Command Line Interface) vagy a grafikus kezelőfelületen (GUI: Graphical User Interface) keresztül kommunikálhat a parancsértelmezővel.

A parancssoros kezelőfelület használata során a felhasználó karakteres környezetben kiadott parancsokkal közvetlenül a rendszerrel kommunikál. A rendszer végrehajtja a parancsot, amelynek végeredményéről általában szöveges kimenetet ad. A grafikus kezelőfelület lehetővé teszi a felhasználó számára, hogy egy grafikus, multimédiás és szöveges elemeket egyaránt használó környezetben kommunikáljon a rendszerrel. Az alapvető műveletek elvégzése a képernyő grafikus elemeivel lehetséges. A grafikus kezelőfelület sokkal könnyebben használható a parancssoros kezelőfelületnél, és a rendszerben rejlő lehetőségek kihasználása is kevesebb tudást igényel. Ebből kifolyólag meglehetősen sokan használják a grafikus kezelőfelületet. A legtöbb operációs rendszer egyaránt biztosít grafikus és parancssoros kezelőfelületet.

Az operációs rendszer teljesen szabadon rendelkezhet a helyi hardver-erőforrásokkal. Az operációs rendszereket egyszerre csak egy felhasználóval történő munkára tervezték, de a felhasználó számára biztosítják több feladat egyidejű elvégzését. Az operációs rendszer nyomon követi, hogy melyik alkalmazás mely erőforrásokat veszi igénybe.

A nem közvetlenül a számítógép-rendszerhez csatlakoztatott erőforrásokkal történő munkához olyan speciális szoftver szükséges, amely lehetővé teszi adatok küldését és fogadását az eszköz és a hálózat között. Az átirányítóként ismert szoftver egyes operációs rendszerek szerves részét képezi, míg másokban hálózati ügyfélként külön kell telepíteni. Az átirányítási funkcióval az operációs rendszer hálózati operációs rendszerré (NOS) válik.

A hálózati operációs rendszer összetett ütemezési és felhasználókezelési programokat biztosít, amelyek lehetővé teszik, hogy egy eszköz erőforrásokat osszon meg több felhasználó között, valamint úgy kezelje a hálózati erőforrásokat, mintha közvetlenül csatlakoztatott eszközök lennének.

2.1.2 Az operációs rendszer követelményei

Napjainkban számos különböző operációs rendszer elérhető a piacon. Az alábbi lista a főbb típusokat és néhány példát tartalmaz:

- Microsoft Windows: XP, Vista, 2003 Server
- UNIX-alapú: IBM AIX, Hewlett Packard HPUX és Sun Solaris
- BSD - Free BSD
- Linux-alapú (számos változatban)
- Macintosh OS X
- További nem UNIX-alapú rendszerek: IBM OS/400, z/OS

Bár a fenti operációs rendszerek többségének használatához szükséges a kereskedelmi licenc megvásárlása és elfogadása, azért az operációs rendszerek világában számos más licencelési forma is létezik, mint például a GPL (GNU General Public Licence - GNU Általános Nyilvános Licenc).

Kereskedelmi licenc esetén rendszerint a felhasználó nem módosíthatja az operációs rendszer kódját. A Windows XP, a Mac OS X és a Unix egyaránt példa a kereskedelmi célú operációs rendszerekre.

Ezzel szemben a nyílt forráskód lehetővé teszi a végfelhasználók számára, hogy a jobb használhatóság érdekében változtassanak és javítsanak a kódon. Az elterjedt nyílt forráskódú operációs rendszerek közé tartozik a Linux és a BSD.

	Kereskedelmi licensz	GPL licensz
Hozzáférés	Korlátozó jellegű és megszabja, hogy a végfelhasználók mit tehetnek a forráskóddal	Mindenki számára teljeskörű hozzáférést nyújt a forráskódhoz, így mindenki részt vehet a termék fejlesztésében.
Költségek	A bevezetés mértékétől függően igen költséges is lehet (például egy hálózat minden ügyfélszámítógépéhez meg kell vásárolni a Windows XP licenszet).	Általában megjelennek ingyenes kiadásai (például Linux alapú operációs rendszerek többsége telepíthető bármennyi számítógépre).
Fejlesztési ciklus	A fejlesztés a gyártó által meghatározott szigorú ütemezés szerint zajlik. Új verzió viszonylag ritkán jelenik meg.	A fejlesztés ütemezése kevésbé szigorú. Viszonylag gyakran végeznek változtatásokat a terméken.
Támogatás	Kiépített támogatási szolgáltatás tartozik hozzá, ami díj ellenében vehető igénybe.	Általában nincs kiépített támogatási rendszer, helyette közösségi alapon, más felhasználók által biztosított segítségnyújtás jellemzi.

Az operációs rendszerek működéséhez meghatározott mennyiségű hardver-erőforrásra van szükség. A gyártó által meghatározott elvárások az alábbiakat tartalmazzák:

- RAM mennyisége
- Szükséges merevlemez-terület
- Processzor típusa és sebessége
- Képernyőfelbontás

A gyártó gyakran meghatározza a minimális mellett az ajánlott hardverigényt is. Minimális hardverigény mellett a rendszerteljesítmény általában gyenge, amely kizárólag az operációs rendszer alapvető működéséhez elég. Rendszerint érdemesebb az ajánlott konfigurációt választani, amely már megfelelő támogatást nyújt az általánosan használt alkalmazások működéséhez is.

Az operációs rendszer képességeinek teljes kiaknázásához további hardver-erőforrások szükségesek, mint például hangkártya, hálózati csatoló, modem, mikrofon és hangszórók. A legtöbb operációs rendszer fejlesztője számos hardvereszközt tesztel, és tanúsítvánnyal igazolja azok kompatibilitását az adott operációs rendszerrel. Vásárlás és telepítés előtt mindig ellenőrizzük, hogy az adott hardver rendelkezik-e tanúsítvánnyal az adott rendszerhez.

2.1.3 Az operációs rendszer kiválasztása

Egy adott környezetben leginkább megfelelő operációs rendszer kiválasztásához számos szempontot kell figyelembe venni.

Első lépésként meg kell bizonyosodni arról, hogy a kiszemelt operációs rendszer teljes mértékben megfelel a végfelhasználó igényeinek. Meg kell vizsgálni, hogy lehetővé teszi-e az ügyfél által használni kívánt programok futtatását, valamint biztonság és funkcionalitás terén is teljesíti-e az elvárásokat.

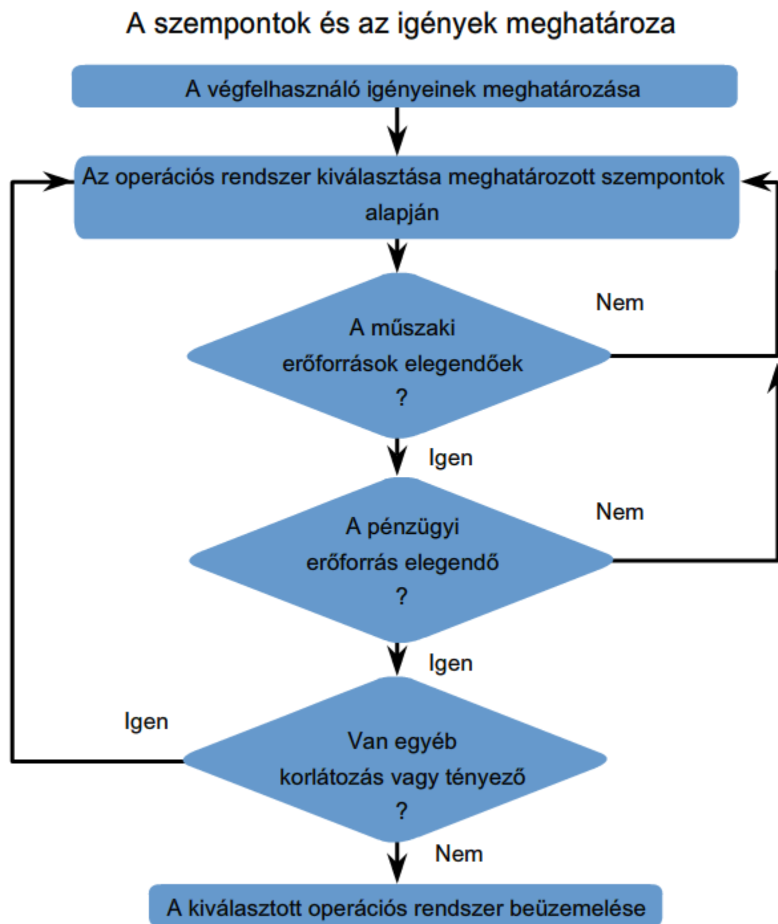
Ezután ellenőrizni kell, hogy a rendelkezésre álló hardver-erőforrások elegendőek-e az operációs rendszer futtatásához. Ilyen alapvető hardverelem a memória, a processzor és a merevlemez-terület, vagy a perifériák közül a lapolvasó, a hangkártya, a hálózati csatoló és a külső meghajtók.

A fentieken túl megfontolandó, hogy az operációs rendszer működtetése és karbantartása milyen emberi erőforrásokat igényel. Üzleti környezetben előfordulhat, hogy egy vállalat mindössze egy vagy két operációs rendszer használatát javasolja, más operációs rendszerek telepítését pedig nem ajánlja vagy egyenesen tiltja. Otthoni környezetben fontos szempont lehet, hogy az operációs rendszerhez tartozik-e bármikor elérhető terméktámogatási szolgáltatás.

Amikor arról döntünk, hogy melyik operációs rendszert válasszuk, akkor mindig figyelembe kell venni a teljes bekerülési költséget (TCO - total cost of ownership). Ez nem csupán a beszerzési és telepítési, hanem a felmerülő támogatási költségeket is magában foglalja.

További szempont lehet a döntéshozatalban az operációs rendszer hozzáférhetősége. Akadhat olyan ország vagy vállalat, ahol egy adott operációs rendszer kizárólagos használatát írják elő, és az is előfordulhat, hogy bizonyos technológiák használatát tiltják. Ilyen helyzetben még akkor sem választhatjuk az utóbbi kategóriába tartozó operációs rendszert, ha az egyébként a célnak tökéletesen megfelelne.

Az operációs rendszer kiválasztása során mindezen szempontokat figyelembe kell venni.



2.2 Az operációs rendszer telepítése

2.2.1 Az operációs rendszer telepítési módjai

Az operációs rendszer telepítése a merevlemez egy meghatározott részére, egy ún. partícióra történik. Az operációs rendszer telepítésének különböző módjai vannak. A kiválasztott módszer a rendszer hardverösszetevőitől, a telepítendő operációs rendszertől és a felhasználói igényektől függ. Egy új operációs rendszer telepítésekor általában négy lehetőség van.

Tiszta telepítés

Tiszta telepítés általában akkor történik, ha új rendszert alakítunk ki, vagy nincs meg az új verzióra történő frissítés lehetősége a jelenlegi operációs rendszerről. Ez a módszer törli az összes adatot arról a partícióról, amelyre az operációs rendszert telepítjük, így a folyamat végén a szoftveralkalmazásokat is újra kell telepíteni. Új számítógép-rendszer esetében tiszta telepítés szükséges. Szintén tiszta telepítést kell végrehajtani, ha a meglévő operációs rendszer valamilyen módon megsérült.

Frissítés

Ha azonos operációs rendszer platformon maradunk, akkor általában lehetséges az újabb verzióra történő frissítés. A frissítés során a rendszerbeállítások, az alkalmazások és az adatok is megmaradnak. Tulajdonképpen csak a régi operációs rendszer fájljait írjuk felül az újakkal.

Több operációs rendszer indításának lehetősége (multi-boot)

Egynél több operációs rendszer is telepíthető a számítógépre, amelyek közül a rendszerindítás során választhatunk. Mindegyik operációs rendszer külön partícióra kerül, saját fájlokkal és konfigurációs beállításokkal. A rendszerindítás során a felhasználó egy menü segítségével választhatja ki a kívánt operációs rendszert. Egyszerre csak egy operációs rendszer futhat, amely kizárólagos felügyeletet gyakorol a hardver felett.

Virtualizáció

A virtualizáció általában kiszolgálókon alkalmazott technika, amely virtuális gépek létrehozásával lehetővé teszi több operációs rendszer futtatását egyazon hardveren. Ebben az esetben ugyanazon a fizikai erőforráson több logikai erőforrás működik.

2.2.2 Az operációs rendszer telepítésének előkészítése

A sikeres telepítés biztosítéka a folyamat megkezdése előtt készített ellenőrzőlista:

1. Ellenőrizzük, hogy minden hardver kompatibilis a kiválasztott operációs rendszerrel.

2. Ellenőrizzük, hogy a hardver-erőforrások biztosan kielégítik a minimális követelményeket.

3. Ellenőrizzük, hogy rendelkezésre áll-e a megfelelő telepítőkészlet! A jelenlegi operációs rendszerek eltérő méreteiből adódóan ez vagy CD-k vagy DVD-k formájában áll rendelkezésre.

4. Amennyiben az operációs rendszer telepítése meglévő adatokat tartalmazó rendszerre történik: (a) Rendszerdiagnosztikai eszközök és segédprogramok használatával bizonyosodjunk meg a jelenlegi operációs rendszer megfelelő állapotáról, vírus- és kémprogrammentességéről; (b) Készítsünk biztonsági mentést minden fontos fájlról!

5. Tiszta telepítés végrehajtása előtt ellenőrizzük, hogy a szükséges szoftveralkalmazások is rendelkezésre állnak-e!

A folyamat megkezdése előtt meg kell határozni a felhasználói igényeket legjobban kielégítő partíciószerkezetet.

Az adatbiztonság növelésének egyik módja, ha a merevlemezt több partícióra osztjuk. A szakemberek többsége tiszta telepítés esetén előnyben részesíti külön-külön partíció létrehozását az adatoknak, illetve az operációs rendszernek. Ez a struktúra lehetővé teszi az operációs rendszer új verzióra történő frissítését az adatvesztés veszélye nélkül, valamint egyszerűsíti az adatfájlok biztonsági mentését és visszaállítását.

Szintén szükséges a használandó fájlrendszer típusának meghatározása. A fájlrendszer az operációs rendszer által használt módszer a fájlok kezelésére. Számos különböző fájlrendszer létezik. Ezek közül a legelterjedtebbek: FAT 16/32, NTFS, HPFS, ext2, ext3. Minden operációs rendszert egy vagy több

fájlrendszerrel való együttműködésre terveztek, ugyanakkor minden fájlrendszer különböző előnyöket kínál. A pozitív jellemzők mérlegelésével alaposan meg kell fontolnunk, hogy melyik rendszert használjuk.

Habár léteznek eszközök, amelyek a telepítés után is képesek a partíciószerkezet és a fájlrendszer megváltoztatására, használatuk lehetőség szerint mégis kerülendő. A merevlemez fájlrendszerének vagy partíciószerkezetének megváltoztatása adatvesztést eredményezhet. Körültekintő tervezéssel elkerülhetjük ezt.

2.2.3 A számítógép beállítása a hálózati munkához

Az operációs rendszer telepítését követően a számítógép beállítható úgy, hogy képes legyen a hálózaton keresztül kommunikálni. A hálózat egymással összekapcsolt eszközök (pl.: számítógépek) csoportja, információ- és erőforrás-megosztás céljából. A megosztott erőforrások közé tartozhatnak nyomtatók, dokumentumok és internetkapcsolatok is.

Ahhoz, hogy egy számítógép fizikailag kapcsolódjon a hálózathoz, egy hálózati csatoló (NIC - Network Interface Card) szükséges. A hálózati csatoló olyan hardverelem, amely lehetővé teszi egy számítógép hálózati közeghez való csatlakozását. Létezik alaplapra integrált és külön, bővítőkártyaként telepíthető változata is.

Ahhoz, hogy a számítógép részt vehessen a hálózati munkában, a fizikai kapcsolódáson túl az operációs rendszer megfelelő beállítása is szükséges. A legtöbb korszerű hálózat kapcsolódik az Internethez, és az Interneten keresztül adatot küld és fogad. Minden egyes hálózatba kötött számítógép azonosításához szükség van egy IP-címre, valamint egyéb információkra. Az IP-konfiguráció három részből áll, amelyek helyes beállítása nélkül nem lehetséges adatküldés és -fogadás a hálózatban. A három rész:

IP-cím - a számítógépet azonosítja a hálózatban.

Alhálózati maszk - a hálózat azonosítására szolgál, amelyhez a számítógép kapcsolódik.

Alapértelmezett átjáró - azt az eszközt azonosítja, amelyen keresztül a számítógép kapcsolódik az internethez vagy egy másik hálózathoz.

A számítógép kaphat IP-címet manuálisan, vagy egy másik eszköztől automatikusan.

Manuális IP-konfiguráció

Manuális konfiguráció esetén a szükséges értékeket álalában a hálózati rendszergazda adja meg a billentyűzetről. Az így megadott IP-címet statikus címnek nevezzük. A számítógéphez mindig ez a cím lesz hozzárendelve.

Dinamikus IP-konfiguráció

A számítógép beállítható úgy, hogy a hálózati konfigurációs adatokat dinamikusan kapja meg. Ilyenkor a számítógép a hálózat egy másik eszköze által kijelölt címhalmazból igényelhet egyet magának. Amennyiben a számítógép már nem tart igényt az adott címre, visszaadja, hogy egy másik számítógép szintén használhassa.

2.2.4 Számítógépnév

Néhány hálózati operációs rendszer az IP-címeken túl számítógépekhez megadott neveket is használ. Ebben az esetben minden egyes rendszernek saját névvel kell rendelkeznie.

A számítógépnév használatával a felhasználók kényelmesebben érhetik el a megosztott erőforrásokat (pl.: mappákat és nyomtatókat).

A hálózati rendszergazda feladata, hogy olyan elnevezési sémát dolgozzon ki, amely utal egy adott eszköz típusára és/vagy helyére. Például a PRT-CL-Eng-01 név jelölheti a Mérnöki Osztály (Engineering Department) első színes lézernyomtatóját.

Az egyes eszközök nevét manuálisan kell megadni, bár léteznek a folyamat automatizálását segítő eszközök. Az elnevezés során megadható a számítógép leírása is, amely bővebb információt tartalmazhat az eszköz helyéről vagy feladatáról.

2.2.5 Hálózati név- és címvezérlés

Ahogy a hálózat mérete és összetettsége is nő, egyre nagyobb jelentősége van a jól átgondolt tervezésnek, a logikus felépítésnek és a megfelelő dokumentálásnak.

Számos szervezet saját névadási és címzési konvenciót alakít ki, amely a hálózati karbantartó személyzet által használható útmutatásokat és szabályokat tartalmaz. A számítógépnév megadásánál egyedi, következetes és beszédes neveket kell használni. Ez alapján könnyen meghatározható egy eszköz típusa, feladata, helye és sorszáma. Az egyes eszközökhöz tartozó IP-címeknek is egyedieknek kell lenniük.

A megfelelően dokumentált, következetes névadási és címzési konvenciók jelentősen egyszerűsítik a munkatársak képzését, a hálózatfelügyeleti folyamatokat és a problémák esetén felmerülő hibaelhárítást.

2.3 Az operációs rendszer karbantartása

2.3.1 Mikor és miért alkalmazunk javításokat?

Fontos, hogy az operációs rendszert és az alkalmazásokat is folyamatosan napra készen tartsuk a legújabb javítások alkalmazásával.

A javítás olyan kódrészlet, amely egy alkalmazás vagy operációs rendszer ismert problémáját megszünteti vagy funkcionalitását bővíti. A felfedezett biztonsági rést vagy problémát megszüntető javításokat általában a gyártó teszi elérhetővé.

Számítógépeinket folyamatosan frissítsük a legújabb javításokkal, hacsak nincs komoly okunk arra, hogy ne így tegyünk. Ritkán előfordulhat, hogy egy javítás negatív hatással van egy másik rendszerkomponens működésére. Mielőtt alkalmaznánk egy javítást, tájékozódjunk a hatásairól. Ez az információ általában megtalálható a gyártó weboldalán.

2.3.2 Az operációs rendszerhez kiadott javítások alkalmazása

Az operációs rendszerhez kiadott javítások többféle módon telepíthetők, a rendszertől és a felhasználói igényektől függően. A frissítések letöltéséhez és telepítéséhez az alábbi lehetőségek állnak rendelkezésre:

Automatikus telepítés

Az operációs rendszer konfigurálható úgy, hogy automatikusan, felhasználói beavatkozás nélkül kapcsolódjon a gyártó weboldalához, majd letöltse és telepítse a kisebb frissítéseket. A frissítés folyamata ütemezhető a bekapcsolt számítógép üresjárataihoz.

Engedélyhez kötött

A felhasználók egy része saját maga akarja eldönteni, hogy alkalmaz-e egy adott javítást. Ezzel a lehetőséggel általában azok a felhasználók élnek, akik pontosan tisztában vannak az egyes javítások rendszerteljesítményre gyakorolt hatásával. A rendszer beállítható úgy, hogy értesítse a felhasználót a megjelenő új javításokról. Ekkor a felhasználó dönt a kérdéses javítás letöltéséről és telepítéséről.

Kézi

A nagyobb kódrészek cseréjével járó frissítéseket érdemes manuálisan telepíteni. Ezeket a javítócsomagnak (angolul support pack-nek) is nevezett frissítéseket egy alkalmazás vagy egy operációs rendszer problémáinak megszüntetésére, esetleg funkcionalitásának bővítésére tervezik. Letöltésükhöz és telepítésükhöz a végfelhasználónak általában el kell látogatnia egy weboldalra, de a gyártótól kapott CD-ről is telepíthetők.

2.3.3 Alkalmazásokhoz kiadott javítások és frissítések

Az alkalmazásokhoz is szükség van javításokra és frissítésekre. A javításokat általában a gyártó teszi elérhetővé, hogy megszüntesse azokat a biztonsági réseket, amelyek a program helytelen működéséhez vezethetnek.

A böngészők és az irodai szoftverek, mint például a szövegszerkesztők, táblázatkezelők és adatbázis-kezelők, a hálózati támadások kedvelt célpontjai. A biztonsági kockázatot jelentő kód javításához frissíteni kell ezeket az alkalmazásokat. A gyártó díjmentesen is kiadhat a termék funkcionalitását javító frissítéseket.

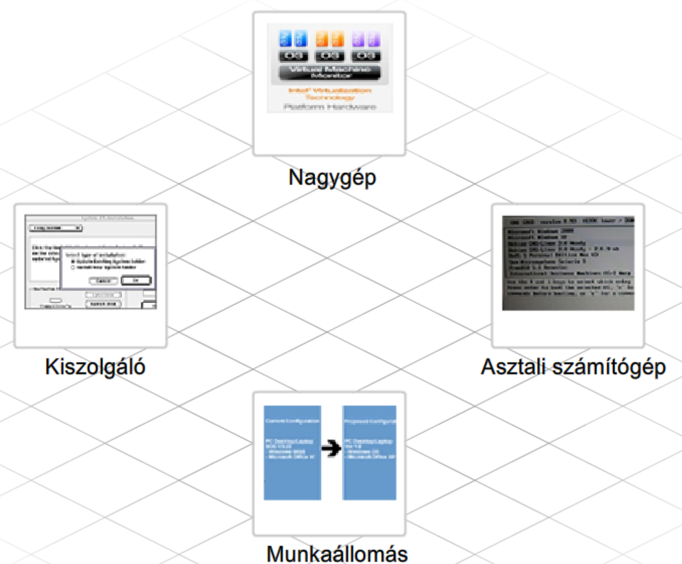
Az operációs rendszerhez és az alkalmazásokhoz kiadott frissítések általában elérhetők a gyártó weboldaláról. A telepítési folyamat köthető engedélyhez, illetve igényelheti a frissítéshez szükséges szoftverek meglétét. A telepítés során további, frissítést támogató programok is települhetnek. A webes frissítések automatikusan letölthetők az Internetről, és telepíthetők a rendszerre.

2.4 A fejezet összefoglalása



- Az operációs rendszer (OS) a legfontosabb szoftver a PC-n. Feladata, hogy minden komponens és szoftveralkalmazás megfelelően együttműködjön.
- A rendszermag közvetlenül a hardverrel, a parancsértelmező pedig az alkalmazásokkal és a felhasználóval kommunikál. A felhasználó a parancssoros vagy a grafikus felhasználói felületen keresztül kommunikál a parancsértelmezővel.
- A hálózati operációs rendszer (NOS) lehetővé teszi, hogy egy eszköz erőforrásokat osszon meg több felhasználó között, valamint úgy kezeli a hálózati erőforrásokat, mintha azok közvetlenül csatlakoznának. A hálózati operációs rendszer számára az adatküldést és -fogadást biztosító szoftvert átirányítónak nevezik.

- Készítsünk ellenőrzőlistát egy új operációs rendszer telepítése előtt.
- Az operációs rendszer telepítése egy partícióra történik, amely a merevlemez egy meghatározott területe. Még az operációs rendszer telepítése előtt döntsük el, milyen módon szervezzük a partíciókat.
- Ahhoz, hogy egy számítógép csatlakozhasson a hálózathoz, szükség van egy hálózati csatolóra, megfelelően konfigurált IP-címmel, alhálózati maszkkal és alapértelmezett átjáróval.
- A hálózatnak alaposan megtervezettnek, logikusan szervezettnek és megfelelően dokumentáltnak kellene lennie.



- **Az operációs rendszert és a szoftveralkalmazásokat is naprakészen kell tartani a legújabb kiadásokkal, frissítésekkel és javításokkal.**
- A javítás olyan programkódrészlet, amely kijavít egy problémát vagy bővíti az operációs rendszer képességeit. Az operációs rendszer konfigurálható úgy, hogy automatikusan, felhasználói beavatkozás nélkül kapcsolódjon a gyártó weboldalához, majd letöltse és telepítse a kisebb frissítéseket.
- A javítócsomagok az operációs rendszerhez kiadott nagyobb frissítések.
- Az alkalmazások szintén igényelhetnek javításokat és frissítéseket a szoftverben felfedezett biztonsági rések megszüntetéséhez.
- Az alkalmazásokhoz tartozó javítások általában megtalálhatók a gyártó weboldalán.



3. Kapcsolódás a hálózathoz

3.1 Bevezetés a hálózatokba

3.1.1 Mi a hálózat?

Sokféle hálózat létezik, melyek különböző szolgáltatásokat biztosítanak számunkra. A nap folyamán valaki telefonál, megnéz egy TV műsort, rádiót hallgat, megkeres valamit az Interneten vagy videojátékot játszik egy másik országban tartózkodó személlyel. Ezeket a tevékenységeket robusztus és megbízható hálózatok teszik lehetővé. A hálózatok biztosítják, hogy emberek és eszközök kapcsolódjanak össze, függetlenül attól, hogy a világ mely pontján vannak. A legtöbben anélkül használják a hálózatokat, hogy ismernék a működésük módját, vagy belegondolnának abba, hogy mi lenne, ha nem léteznének.

Az 1990-es években és azt megelőzően, a kommunikációs technológia különálló, dedikált hálózatokat használt a hang-, videó- és adat kommunikációra. Mindegyik hálózatban másfajta eszköz biztosította a kapcsolódást. A telefonok, a televíziók és a számítógépek sajátos technológiákat és különálló, dedikált hálózatokat használtak a kommunikációhoz. De mi van akkor, ha az emberek azonos időben szeretnének hozzáférni ezekhez a hálózati szolgáltatásokhoz, esetleg egyetlen eszközt akarnak csak használni?

Az új technológiák egy olyan újfajta hálózatot hoztak létre, amely nem korlátozódik egyetlen szolgáltatás biztosítására. A dedikált hálózatokkal szemben, ezek az új konvergált hálózatok képesek hangot, videót és adatokat is szállítani ugyanazon a kommunikációs csatornán vagy hálózaton keresztül.

A piacon új termékek jelennek meg, amelyek kihasználják a konvergált információs hálózatok képességeit. Ma már az emberek élő videó adásokat nézhetnek a számítógépeiken, telefonálhatnak az Interneten, vagy televíziójukat használva kereshetnek az Interneten. A konvergált hálózatok teszik lehetővé mindezt.

Ebben a tananyagban a hálózat fogalma alatt mindvégig ezt az új, többcélú, konvergált információs hálózatot fogjuk érteni.

3.1.2 A hálózatok előnyei

A hálózatok mérete a legegyszerűbb két számítógépes hálózattól egészen a több millió eszközt tartalmazó hálózatokig terjedhet. A kisméretű irodákban, az otthoni irodákban és az otthonokban telepített hálózatokat SOHO hálózatoknak nevezik. A SOHO hálózatok lehetővé teszik, hogy néhány számítógép között erőforrásokat (nyomtatókat, dokumentumokat, képeket, zenéket stb.) osszunk meg.

Az üzleti életben kiterjedt hálózatokat használnak hirdetési célra, termékek eladásához, alapanyag rendeléshez vagy az ügyfelekkel történő kommunikációhoz. A hálózatokon keresztüli kommunikáció általában jóval hatékonyabb és olcsóbb, mint a hagyományos levelezéshez vagy a nagy távolságú telefonhíváshoz hasonló tradicionális kommunikációs megoldások. A hálózatok gyors kommunikációt



tesznek lehetővé (példaként az elektronikus levelezést vagy az azonnali üzenetküldést említhetjük), és megfelelő kiszolgálókon keresztül biztosítják az információ tárolását, az adatok elérését is.

Az üzleti és SOHO hálózatok általában egyetlen kapcsolattal rendelkeznek az Internet felé. Ezt a megosztott kapcsolatot használják közösen az egyes állomások az Interneten történő kommunikációhoz. Az Internetet a "hálózatok hálózatának" tartják, mivel szó szerint sok-sok ezer egymáshoz kapcsolt hálózatból épül fel.

A hálózatok és az Internet használatának módjai:

- Zene- és videó-megosztás
- Kutatás és on-line tanulás
- Barátokkal való társalgás
- Vakációtervezés
- Ajándék és áruvásárlás

Milyen további módokon használhatják az emberek a hálózatokat és az Internetet a mindennapi életükben?

3.1.3 Alapvető hálózati összetevők

A hálózatok sokfajta összetevőből épülnek fel. Ezek közé sorolhatjuk például a személyi számítógépeket, a kiszolgálókat, a hálózati eszközöket és a kábeleket. Az összetevőket négy nagy csoportba sorolhatjuk:

- Állomások
- Megosztott perifériák
- Hálózati készülékek
- Hálózati átviteli közegek

A legismertebb hálózati összetevők az állomások és a megosztott perifériák. Az állomások azok az eszközök, melyek üzenetet küldenek és fogadnak közvetlenül a hálózaton keresztül.

A megosztott perifériák nem közvetlenül, hanem az állomásokon keresztül kapcsolódnak a hálózathoz. Ebben a helyzetben az állomás a felelős a periféria hálózaton történő megosztásáért. Az állomáson futó speciális szoftver teszi lehetővé, hogy a felhasználók a hálózaton keresztül használják az állomáshoz kapcsolt perifériát.

A hálózati eszközöket, éppúgy mint a hálózati átviteli közegeket, az állomások összekapcsolására használják.

Néhány eszköztípus több szerepben is megjelenhet, attól függően, hogy miként van csatlakoztatva. Az állomáshoz csatlakoztatott helyi nyomtatót például perifériaként emlegetjük, de a hálózathoz direkt módon csatlakoztatott, és a hálózati kommunikációban közvetlenül résztvevő nyomtatót már állomásnak tekintjük.

3.1.4 Számítógépes szerepek a hálózatban

Minden olyan számítógépet állomásnak nevezünk, amely csatlakozik a hálózathoz és közvetlenül részt vesz a hálózati kommunikációban. Az állomások üzeneteket küldhetnek és fogadhatnak a hálózaton keresztül. A modern hálózatokban az állomások lehetnek ügyfelek, kiszolgálók vagy mind a kettő egyszerre. A számítógépre telepített program határozza meg, hogy milyen szerepet játszhat a számítógép.

A kiszolgálók azok az állomások, melyekre olyan program van telepítve, mely lehetővé teszi, hogy más hálózati állomásoknak olyan jellegű információk elérését biztosítsák, mint például elektronikus levelek vagy web oldalak. Minden szolgáltatás egy különálló kiszolgálóprogramot igényel. Web kiszolgálóprogramra van szükség például ahhoz, hogy egy állomás web-szolgáltatást tudjon nyújtani a hálózat számára.

Az ügyfelek azok az állomások, melyekre olyan szoftver van telepítve, ami lehetővé teszi, hogy információt kérjen a kiszolgálóktól, majd megjelenítse azt. Az ügyfélprogramra példa a web böngészők közé tartozó Internet Explorer.

A kiszolgálóprogrammal ellátott számítógép szolgáltatásokat biztosíthat egyszerre egy vagy több ügyfélnek.

Egy számítógép több különböző típusú kiszolgálóprogramot tud futtatni egyszerre. Otthoni- vagy kisvállalati környezetben szükség lehet arra, hogy ugyanaz a számítógép legyen a fájlkiszolgáló, webkiszolgáló és az elektronikus levelezés kiszolgálója is egyben.

Egyetlen számítógép többféle ügyfélprogramot is tud futtatni. Minden igényelt szolgáltatáshoz szükség van egy ügyfélprogramra (kliensprogramra). Több feltelepített ügyfélprogrammal egy állomás több kiszolgálóhoz tud kapcsolódni egyszerre. Egy felhasználó például megnézheti az elektronikus leveleit, és letölthet egy weboldalt, miközben azonnali üzenetküldőn beszél, és internetes rádiót hallgat.

3.1.5 Egyenrangú (peer-to-peer) hálózatok

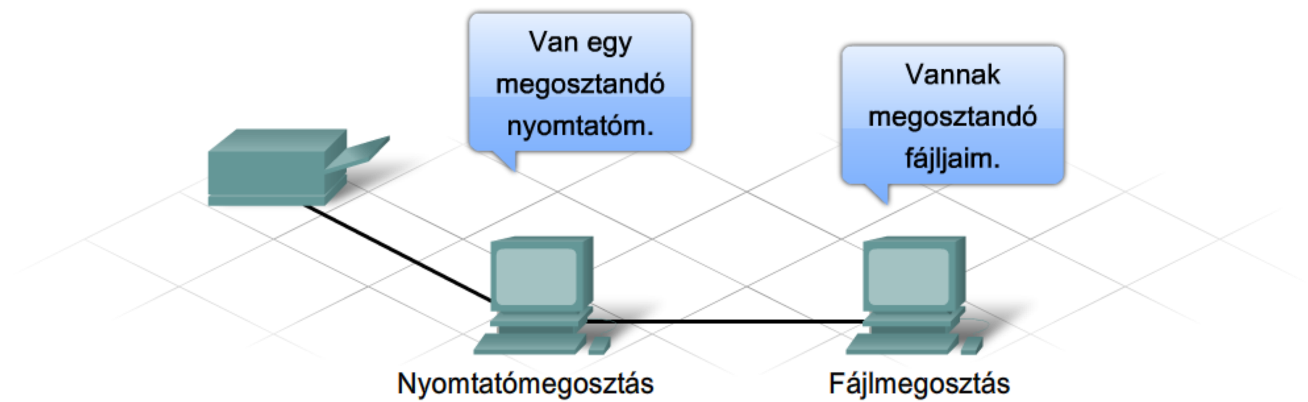
Az ügyfél- és kiszolgálóprogramok általában külön számítógépeken futnak, de az is lehetséges, hogy egy számítógép mind a két szerepet egyszerre töltse be. Kisvállalati és otthoni hálózatokban sok számítógép működik kiszolgálóként és ügyfélként is egyben. Az ilyen hálózatot egyenrangú hálózatnak nevezzük.

A legegyszerűbb egyenrangú hálózat két számítógépet tartalmaz, melyek vezetékkel vagy vezeték nélküli technológiával közvetlenül kapcsolódnak egymáshoz.

Több PC-ből álló, nagyobb egyenrangú hálózatot is létrehozhatunk, de ekkor a számítógépek összekapcsolásához szükség van egy hálózati eszközre, például hub-ra.

A fő hátránya az egyenrangú hálózati környezetnek az, hogy ha az állomás ügyfélként és kiszolgálóként is működik egyszerre, akkor a teljesítménye lecsökkenhet.

Nagyobb vállalatoknál gyakran előfordul, hogy a komoly hálózati forgalmat generáló nagyszámú ügyfélkérés miatt dedikált kiszolgálót kell üzembe állítani.



Az egyenrangú hálózatok előnyei:

- Könnyen konfigurálható
- Kevésbé összetett
- Alacsonyabb költségű, mivel hálózati eszközökre és dedikált kiszolgálókra nincs szükség
- Egyszerű feladatok elvégzésére alkalmas, mint például fájlátvitel és nyomtatómegosztás

Az egyenrangú hálózatok hátrányai:

- Nincs központosított adminisztráció
- Nem biztonságos
- Nem skálázható
- Minden eszköz működhet egyszerre kliensként és kiszolgálóként is, ami csökkentheti a teljesítményüket

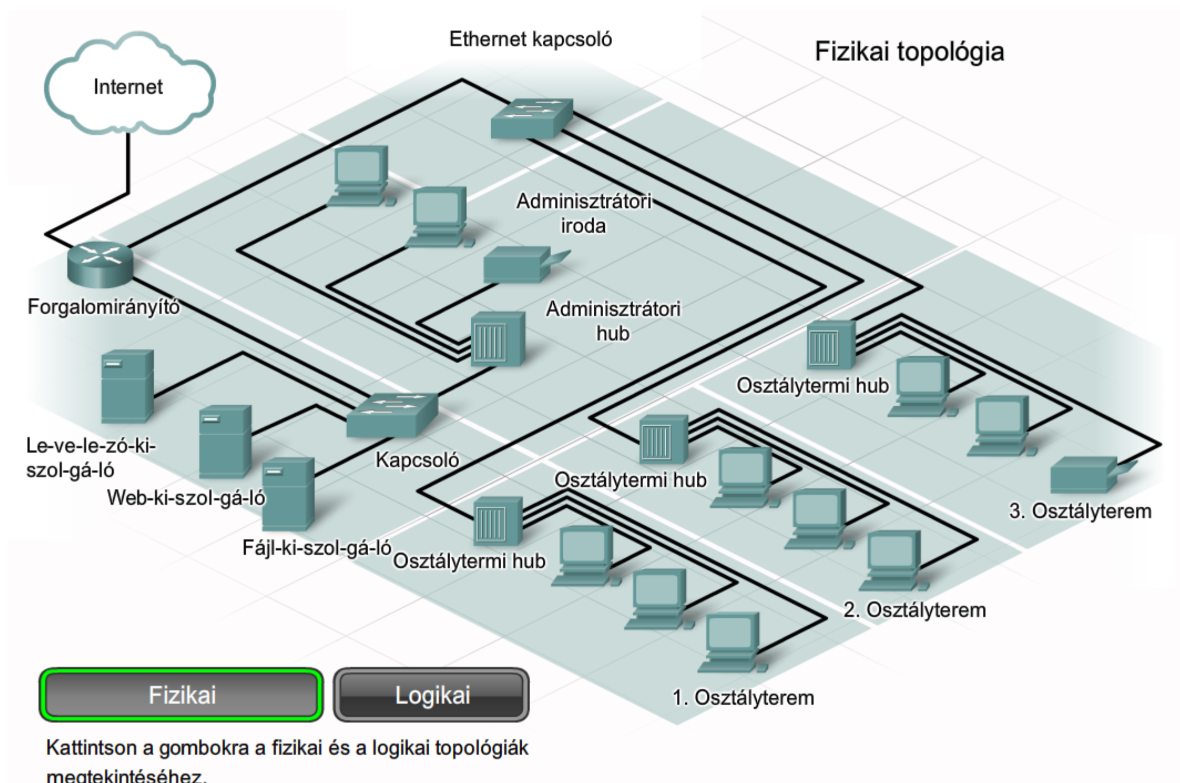
3.1.6 Hálózati topológiák

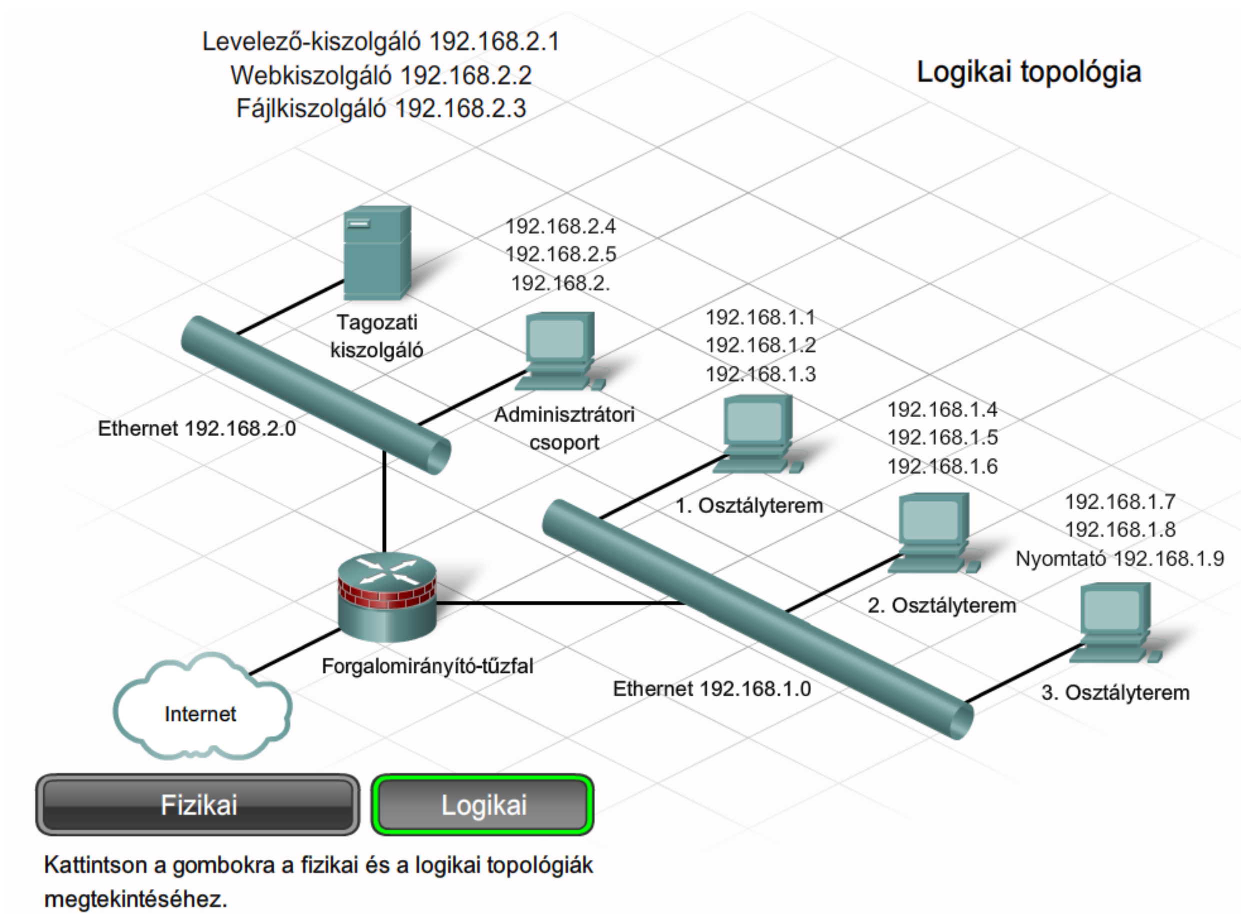
Egy egyszerű, néhány számítógépet tartalmazó hálózatban egyszerű elképzelni, hogy a különböző összetevők hogy csatlakoznak. Ahogy a hálózat nő, egyre bonyolultabb lesz nyomon követni a hálózati összetevők helyét és a hálózati kapcsolódásukat. A vezetékes hálózatokban az összes hálózati állomás összekapcsolásához sok kábelre és hálózati eszközre van szükség.

Amikor a hálózatot telepítik, fizikai topológiai térkép készül, hogy rögzítse, hol és hogyan csatlakoznak az egyes állomások a hálózathoz. A fizikai topológiai térkép azt is megmutatja, hogy a kábelezés hol fut, és az állomásokat csatlakoztató hálózati eszközök hol találhatóak. A topológiai térképen ikonokat használunk a valódi fizikai eszközök ábrázolására. Nagyon fontos a fizikai topológiai térkép karbantartása és frissítése, mivel a naprakész térkép megkönnyíti a hibaelhárítást és a későbbi bővítést.

A fizikai topológiai térképen kívül néha szükséges a hálózati topológia logikai nézete is. A logikai topológiai térképen az alapján csoportosítjuk az állomásokat, ahogyan használják a hálózatot, tekintet nélkül a fizikai elhelyezkedésükre. Állomásneveket, címeket, csoportinformációkat és alkalmazásokat rögzíthetünk a logikai topológiai térképen.

Az ábrák a logikai és a fizikai topológiai térképek közötti különbséget szemlélteti.


Ethernet kapcsoló
Fizikai topológia
Internet
Adminisztrátori iroda
Forgalomirányító
Adminisztrátori hub
Osztálytermi hub
Le-ve-le-zó-ki-szol-gá-ló
Kapcsoló
Osztálytermi hub
Web-ki-szol-gá-ló
3. Osztályterem
Fájl-ki-szol-gá-ló
Osztálytermi hub
2. Osztályterem
Fizikai
Logikai
1. Osztályterem
Kattintson a gombokra a fizikai és a logikai topológiák megtekintéséhez.


Levelező-kiszolgáló 192.168.2.1
Webkiszolgáló 192.168.2.2
Fájlkiszolgáló 192.168.2.3
Logikai topológia
192.168.2.4
192.168.2.5
192.168.2.
Tagozati kiszolgáló
192.168.1.1
192.168.1.2
192.168.1.3
Adminisztrátori csoport
Ethernet 192.168.2.0
192.168.1.4
192.168.1.5
192.168.1.6
1. Osztályterem
192.168.1.7
192.168.1.8
Nyomtató 192.168.1.9
2. Osztályterem
Forgalomirányító-tűzfal
Ethernet 192.168.1.0
3. Osztályterem
Internet
Fizikai
Logikai
Kattintson a gombokra a fizikai és a logikai topológiák megtekintéséhez.

3.2 Kommunikációs alapelvek

3.2.1 Forrás, csatorna, cél

Minden hálózat elsődleges célja hogy biztosítsa az információáramlást. A nagyon korai, primitív emberektől kezdve napjaink legjobb tudósaiig bezárólag, mindenki számára döntő fontosságú az információ másokkal történő megosztása, mivel ez az egyik alapja az emberi előrehaladásnak.

Minden kommunikáció egy üzenettel, másképp nevezve információval kezdődik, amit egy egyén vagy eszköz küld egy másiknak. A technológia fejlődésével folyamatosan változik a módszer, ahogyan az üzeneteket küldjük, fogadjuk és értelmezzük.

Minden kommunikációs módszerben van három közös alkotóelem. Ezek közül az első az üzenet forrása vagy másképpen küldője. Az üzenet forrásai emberek vagy elektronikai eszközök lehetnek, akik vagy amik üzenetet közölnek más egyénekkel vagy eszközökkel. A kommunikáció második alkotóeleme az üzenet célállomása vagy vevője. A célállomás fogadja és értelmezi az üzenetet. A harmadik alkotóelem a csatorna, ami a forrástól a célig biztosítja az utat az üzenet számára.

3.2.2 Kommunikációs szabályok

Két ember közötti tetszőleges kommunikáció esetén rengeteg olyan szabály vagy protokoll van, amit mind a kettőjüknek követni kell ahhoz, hogy az egymásnak küldött üzenetek eljussanak a másik félhez, és a fogadó megértse azokat. A sikeres emberi kommunikációhoz szükséges protokollok az alábbiak:

- A küldő és a fogadó azonosítása
- Megállapodás szerinti közeg vagy csatorna (szemtől szembe, telefon, levél, fénykép)
- Megfelelő kommunikációs mód (beszélt, írásbeli, képekkel ellátott, interaktív, egyirányú)
- Közös nyelv
- Nyelvtani és mondattani struktúra
- A sebesség és a kézbesítés időzítése

Képzelje el, mi történne, ha nem lennének protokollok és szabályok, melyek szabályozzák az emberek közötti kommunikációt! Képesek lennénk megérteni egymást? Képesek lennénk elolvasni azt a bekezdést, ami nem követi a közösen elfogadott protokollokat?

A protokollokat az üzenet forrásának, vevőjének és átvivő csatornájának jellemzői határozzák meg. A szabályok, amit egy adott közegen történő kommunikációhoz alkalmazunk, nem feltétlenül azonosak, ha más közeget használunk. Más szabályok érvényesek például telefonhívás esetén, mint levélváltáskor.

A protokollok definiálják az üzenetküldés és a szállítás részleteit. Ezek a következők:

- Üzenetformátum
- Üzenetméret
- Időzítés
- Beágyazás
- Kódolás
- Szabványos üzenetminta

A számítógépes kommunikációnál is alkalmazzuk azokat a fogalmakat és szabályokat, amelyek megbízhatóvá és érthetővé teszik az emberi kommunikációt.

3.2.3 Üzenetkódolás

Az első lépés az üzenetküldéshez az üzenet kódolása. Az írott szavak, a képek, a beszélt nyelvek mind egyedi kódkészletet, hangokat, gesztusokat, és/vagy szimbólumokat használnak a megosztani kívánt gondolat kifejezésére. A kódolás az a folyamat, melynek során a gondolatokat átalakítjuk az átvitelhez szükséges nyelvre, szimbólumokra vagy hangokra. A dekódolás megfordítja ezt a folyamatot, annak érdekében, hogy értelmezni tudjuk a gondolatot.

Képzeljen el egy személyt, aki a naplementét nézi, és felhív valakit, hogy elmondja neki, milyen szép az elé táruló látvány. Az üzenet közléséhez a küldőnek a gondolatait és észleléseit a naplementéről először szavakká kell konvertálnia, vagyis kódolnia kell. A beszélt nyelv ragozásait és az emberi hangot használva a küldő a szavakat az üzenet továbbítását végző telefonba mondja. A telefonvonal másik végén egy másik ember hallgatja a leírást, fogadja és dekódolja a hangokat, hogy végül maga elé képzelhesse a küldő által leírt naplementét.

A számítógépes kommunikációban is történik kódolás. Két állomás közötti kódolásnak az átviteli közegnek megfelelő formátumúnak kell lennie. A hálózaton át küldött üzenetet először a küldő állomás bitekké konvertálja. Minden bitet hangmintává, fényhullámmá vagy elektromos impulzussá kódol, annak függvényében, hogy milyen hálózati közegen fogja a biteket továbbítani. A célállomás fogadja, és az üzenet értelmezéséhez dekódolja a jeleket.

3.2.4 Üzenetformázás

Meghatározott formátumot és szerkezetet kell használni, amikor egy üzenetet a forrástól a célig akarunk eljuttatni. Az üzenet formátuma az üzenet típusától és az átvitelhez használt csatornától függ.

Az egyik leggyakoribb formája az emberi írásbeli kommunikációnak az írott betű. A magánlevelek egyezményes formája évszázadok óta nem változott. A legtöbb kultúrában a magánlevelek a következő alkotóelemeket tartalmazzák:

- a fogadó azonosítása
- megszólítás vagy üdvözlés
- az üzenet tartalma
- záró mondat
- a küldő azonosítása

A szállításhoz megfelelő formátumot kell alkalmazni, ami levelek esetén a becsomagolás vagy a borítékba helyezés. A borítékon rögzített helyen van a küldő és a fogadó címe. Ha a célcím vagy a formátum helytelen, a levelet nem szállítják el.

Beágyazásnak hívjuk azt a folyamatot, amikor egy üzenetformátumot (levél) egy másik üzenetformátumba (boríték) helyezünk. Amikor a fogadó a folyamatot megfordítja, kicsomagolás történik, a levelet kivesszük a borítékból.

A levél írója megegyezés szerinti formátumot használ annak érdekében, hogy a levelet elszállítsák, és a fogadó megértse az üzenetet. Hasonlóképpen a számítógép-hálózaton küldött üzenet is egy

speciális formázási szabályt követ, hogy elszállítsák és feldolgozzák. Ahogy a levelet borítékba ágyaztuk a szállításhoz, ehhez hasonlóan a számítógépes üzeneteket is beágyazzuk. A hálózaton való továbbítás előtt minden számítógépes üzenetet beágyazunk egy keretnek nevezett speciális formátumba. A keret borítékként funkcionál, tartalmazza a cél- és a forrásállomás címét.

A keret formátumát és tartalmát a küldött üzenet típusa és a közlésre használt csatorna határozza meg. A nem megfelelően formázott üzenetek továbbítása általában nem lehetséges, de az is előfordulhat, hogy megérkezés után a célállomás nem tudja feldolgozni azt.

Cél (fizikai / hardver cím)	Forrás (fizikai / hardver cím)	Start Flag (üzenet kezdet jelző)	Fogadó (cél azonosítója)	Küldő (forrás azonosítója)	Beágyazott adat (bitek)	Keret vége (üzenet vége jelző)
Keret címzés		Beágyazott üzenet				

3.2.5 Üzenet méret

Képzelje el, hogy milyen lenne ezt a tananyagot úgy olvasni, hogy az egész csak egyetlen hosszú mondatból állna. Egy ilyen szöveget nem lenne könnyű olvasni és megérteni. Amikor az emberek egymással kommunikálnak, a küldendő üzenetet általában kisebb részekre, rendszerint mondatokra tördelik. A mondatok nem haladhatják meg azt a méretet, amit a fogadó személy egyszerre fel tud dolgozni. Az egyéni kommunikáció sok kisebb mondatból áll, ezzel biztosítva, hogy az üzenet minden részét fogadja és megértse a címzett.

A fentiekhez hasonlóan, amikor az egyik állomás hosszabb üzenetet küld egy másik állomásnak a hálózaton, szükséges az üzenet kisebb részekre darabolása. A hálózaton érvényben levő, a darabok (keretek) méretét szabályozó szabályok nagyon szigorúak, és a használt csatornától függően eltérőek lehetnek. A túlságosan hosszú vagy rövid keretek nem kerülnek szállításra.

A keretek méretkorlátozásai megkívánják, hogy a forrásállomás a hosszú üzeneteket olyan darabokra tördelje, amik megfelelnek a minimális és a maximális méretre vonatkozó követelményeknek. Minden egyes darabot címzési információval ellátott külön keretbe ágyaznak, majd továbbítják a hálózaton. A fogadó állomás a feldolgozás és az értelmezés előtt az üzeneteket kicsomagolja és összeilleszti.

3.2.6 Üzenetidőzítés

Az egyik tényező, ami hatással van arra, hogy milyen eredményesen lehet fogadni és értelmezni az üzenetet, az időzítés. Az emberek az időzítést arra használják, hogy megállapítsák mikor és milyen gyorsan vagy lassan beszéljenek, valamint hogy mennyit várjanak a válaszra. Ezek megegyezésen alapuló szabályok.

Hozzáférési mód

A hozzáférési mód meghatározza, hogy mikor küldhet valaki üzenetet. Ezek az időzítési szabályok a környezethez igazodnak. Egy ember bármikor képes elkezdeni beszélni. Ebben a környezetben, a beszéd előtt azonban várni kell addig, amíg mindenki más befejezi a beszédet. Ha két ember beszél egyszerre, információütközés történik, és szükséges, hogy mind a ketten abbahagyják és később újrakezdjék a folyamatot. Ezek a szabályok biztosítják a kommunikáció sikerét. Hasonlóképpen ehhez, a számítógépek számára is definiálni kell a hozzáférési módot. A hálózaton az állomásoknak ismerniük kell a hozzáférési módot, hogy tudják mikor kezdhetik az üzenet küldését, és hogyan viselkedjenek, ha hiba történik.

Adatfolyam-vezérlés

Az időzítés arra is hatással van, hogy mennyi információt lehet küldeni és milyen gyorsan. Ha egy ember túlságosan gyorsan beszél, a többieknek nehéz hallani és megérteni az üzenetet. A fogadó személynek ebben az esetben meg kell kérnie a küldőt, hogy lassítson. A hálózati kommunikáció során is előfordulhat, hogy a küldő állomás gyorsabban küld üzenetet, mint ahogyan a célállomás fogadni és feldolgozni tudná azt. A forrás- és célállomások adatfolyam-vezérlést használnak a helyes időzítés jelzésére, ezáltal biztosítva a sikeres kommunikációt.

Válaszidő túllépése

Ha valaki feltesz egy kérdést, és nem hallja a választ elfogadható időn belül, akkor feltételezi, hogy már nem is jön válasz, és ennek megfelelően reagál. Lehet, hogy megismétli a kérdést, de az is lehet, hogy folytatja a párbeszédet. A hálózati állomásoknak szintén vannak szabályai, amik meghatározzák, hogy mennyit kell várni a válaszra, és mit kell csinálni, ha válaszidő túllépés történik.

3.2.7 Üzenet sémák

Vannak olyan helyzetek, mikor csupán egyetlen emberrel szeretnénk valamilyen információt megosztani. Máskor előfordulhat, hogy emberek egy csoportjával, vagy akár egy adott területen lévő összes emberrel szeretnénk egyszerre közölni valamit. A két ember közötti párbeszéd példa az egy-az-egyhez kommunikációs sémára. Amikor fogadók egy csoportjának kell ugyanazt az üzenetet fogadnia, akkor egy-a-többhöz vagy egy-a-mindenkihez üzenetséma érvényesül.

Néha az üzenet küldőjének meg kell győződnie arról, hogy a célnak küldött üzenetét sikeresen kézbesítették. Ebben az esetben elvárás, hogy a fogadó egy nyugtát küldjön vissza a küldőnek. Ha nincs szükség nyugtára, akkor nyugtázatlan üzenetsémáról beszélünk.

A hálózaton az állomások hasonló üzenetsémákat használnak a kommunikációhoz.

Az egy-az-egyhez üzenetsémára az egyedi (unicast) kifejezést használjuk, ami jelzi, hogy csak egyetlen célja van az üzenetnek.

Amikor az állomás egy-a-többhöz sémát használ az üzenetküldéshez, akkor csoportos (multicast) küldésről beszélünk. A csoportos küldés esetén az üzenetet egyszerre továbbítjuk a célállomások egy csoportjának.

Ha a hálózaton egy időben az összes állomásnak meg kell kapnia az üzenetet, akkor ezt az esetet szórásnak (broadcast) nevezzük. A szórás az egy-a-mindenkihez sémát valósítja meg. A fenti sémák



mellett egyes esetekben a fogadónak nem kell megerősítést küldenie (nyugtázatlan üzenetküldés), míg máskor a küldő elvárhatja, hogy visszajelzést kapjon a sikeres kézbesítésről (nyugtázott üzenetküldés).

3.2.8 A kommunikációban használt protokollok

Minden kommunikációt – akár emberi, akár számítógépes – előre lefektetett szabályok, a protokollok irányítják. A protokollokat a forrás, a csatorna, és a cél jellemzői határozzák meg. A fentiek alapján a protokollok definiálják az üzenet formátumára, az üzenet méretére, az időzítésre, a beágyazási módra, a kódolásra és a szabványos üzenetsémára vonatkozó követelményeket.

3.3 Kommunikáció a helyi vezetékes hálózaton keresztül

3.3.1 A protokollok fontossága

A számítógépek, az emberekhez hasonlóan, szabályokat vagy protokollokat használnak a kommunikációhoz.

A protokollok különösen fontosak a helyi hálózaton. Vezetékes környezetben a helyi hálózat alatt egy olyan területet értünk, ahol minden állomásnak „ugyanazt a nyelvet kell beszélnie” vagy számítógépes terminológiát használva „ugyanazt a protokollt kell használnia”.

Ha egy szobában mindenki más nyelven beszél, nem fogják megérteni egymást. Hasonlóképpen, ha a helyi hálózatban levő eszközök nem ugyanazokat a protokollokat használják, nem lesznek képesek kommunikálni egymással.

A vezetékes helyi hálózatban a leggyakrabban használt protokollkészlet az Ethernet.

Az Ethernet protokoll a helyi hálózaton keresztüli kommunikáció számos összetevőjét határozza meg, úgymint az üzenet formátumát, az üzenet méretét, az időzítést, a kódolást és az üzenetsémákat.

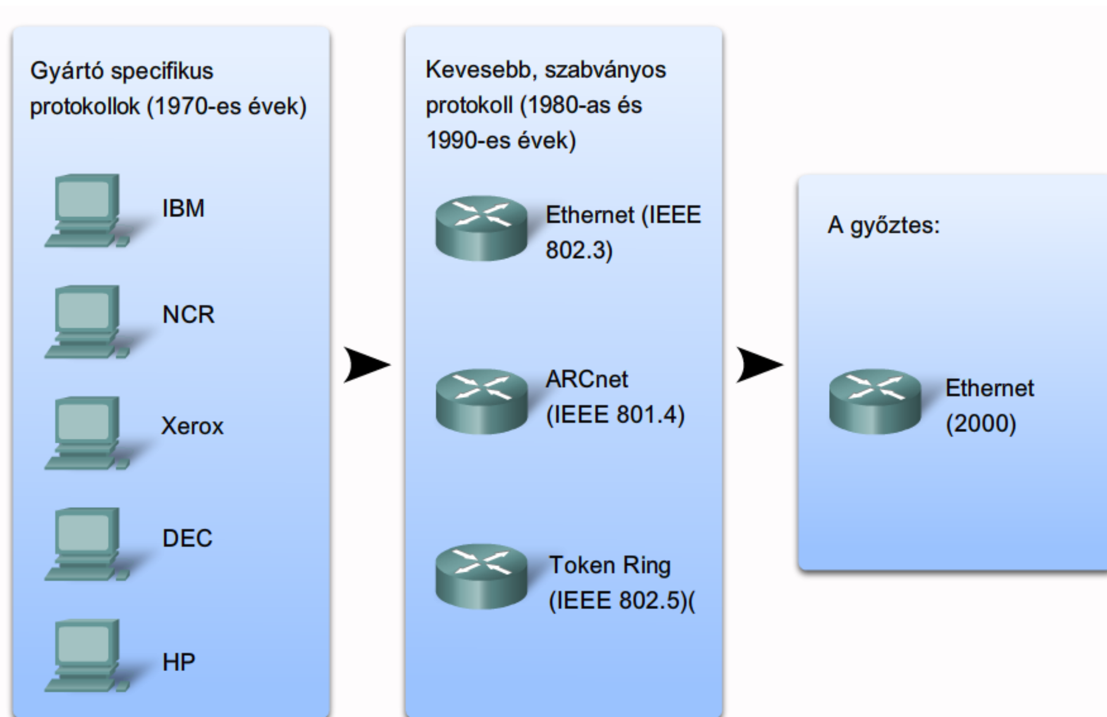
3.3.2 A protokollok szabványosítása

A korai hálózatok idejében minden gyártó a saját módszerét használta a hálózati eszközök összekapcsolására és a hálózati protokollokra. Az egyik gyártótól származó eszköz nem tudott kommunikálni egy másik gyártó eszközével.

Ahogy a hálózatok egyre jobban elterjedtek, szabványokat dolgoztak ki, amik olyan szabályokat definiáltak, amivel a különböző gyártóktól származó hálózati eszközök együtt tudtak működni. A szabványok sokféle előnyt nyújtanak a hálózatok számára:

- Elősegítik a tervezést.
- Egyszerűsítik a termékfejlesztést.
- Támogatják a versenyt.
- Következetes összekapcsolódást biztosítanak.
- Elősegítik az oktatást.
- Biztosítják az ügyfelek számára, hogy több gyártó közül választhassanak.

Helyi hálózatos környezetben nem létezik hivatalos szabványos protokoll, de idővel az egyik technológia, az Ethernet, a többinél gyakoribbá vált, azaz de facto szabvány lett.



A Villamos- és Elektronikai Mérnökök Intézete (IEEE - Institute of Electrical and Electronic Engineers) az a szervezet, ami kezeli a hálózati szabványokat, így az Ethernet és a vezeték nélküli szabványokat is. Az IEEE bizottságok a felelősök a kapcsolatokra, az átviteli közegek követelményeire és a kommunikációs protokollokra vonatkozó szabványok jóváhagyásáért és karbantartásáért. Minden technológiai szabvány kap egy számot, ami azt a bizottságot jelzi, amelyik felelős az adott szabványért. Az Ethernet szabvány a 802.3-as számú bizottsághoz tartozik.

Az Ethernet 1973-as megszületése óta számos új szabvány jött létre a gyorsabb és rugalmasabb technológiai verziók érdekében. Az Ethernet folyamatos fejlődési képessége a fő oka annak, hogy ilyen népszerű lett. Minden Ethernet verzióhoz tartozik egy szabvány. Például a 802.3 100BASE-T a 100 megabites csavart érpárt használó Ethernet szabványt jelöli. A szabvány rövidítése az alábbiakat jelöli:

A 100 a sebességet jelöli Mbit/s-ban.

A BASE mutatja, hogy alapsávi átvitelről van szó.

T jelzi a kábel típusát, ebben az esetben a csavart érpárt.

Az Ethernet korai változatai relatíve lassúak, 10 Mbit/s-ok voltak. A legújabb Ethernet verziók 10 Gbit/s vagy még ennél is nagyobb sebességgel működnek. Hasonlítsa össze, hogy mennyivel gyorsabbak a mai verziók, mint a hagyományos Ethernet hálózatok!

Év	1973	1980	1983
Szabvány	Ethernet	DIX szabvány	IEEE 802.3
Leírás	A Xerox corp.-nál dolgozó Dr Robert Metcalf találta fel az Ethernetet.	A Digital Equipment Corp, az Intel és a Xerox (DIX) kiadta a koaxiális kábelen 10 Mbit/s sebességgel működő Ethernet szabványt.	10 Mbps Ethernet vastag koaxiális kábelen

Év	1985	1990	1993
Szabvány	IEEE 802.3a	IEEE 802.3i	IEEE 802.3j
Leírás	10 Mbps Ethernet vékony koaxiális kábelen	10 Mbps Ethernet csavart érpáron (TP)	10 Mbps Ethernet optikai szálon

Év	1995	1998	1999
Szabvány	IEEE 802.3u	IEEE 802.3z	IEEE 802.3ab
Leírás	Fast Ethernet: 100 Mbps Ethernet csavart érpáron (TP) vagy optikai szálon (különböző szabványok)	Gigabit Ethernet optikai szálon	Gigabit Ethernet csavart érpáron

Év		1999	2002	2006
Szabvány		IEEE 802.3ab	IEEE 802.3ae	IEEE 802.3an
Leírás		Gigabit Ethernet csavart érpáron	10 Gigabit Ethernet optikai szálon (változó szabványok)	10 Gigabit Ethernet csavart érpáron (TP)

3.3.3 Fizikai címzés

Minden kommunikációban a forrást és célt valamilyen módon azonosítani kell. Az emberi kommunikációban a forrást és a célt a nevek azonosítják.

Amikor egy nevet valahol kimondanak, a név tulajdonosa meghallgatja az utána következő üzenetet és válaszol rá. Lehet, hogy a szobában lévő többi ember is hallja az üzenetet, de figyelmen kívül hagyják azt, mivel nem nekik címezték.

Az Ethernet hálózatokban hasonló módszer létezik a forrás- és a célállomás azonosítására. Minden Ethernet hálózathoz csatlakoztatott állomáshoz egy fizikai cím van hozzárendelve, ez szolgál az állomás azonosítására a hálózaton.

Minden Ethernet hálózati interfésznek egyedi fizikai címe van, amit a gyártáskor rendelnek hozzá. Ezt a címet közeghozzáférés-vezérlési (MAC - Media Access Control) címként ismerjük. A hálózat valamennyi forrás- és célállomását egy-egy MAC-cím azonosítja.



Az Ethernet hálózatok kábel alapúak, ami azt jelenti, hogy rézvezeték, vagy optikai kábel köti össze az állomásokat és a hálózati eszközöket. Ez az a csatorna, amit az állomások közötti kommunikációhoz használunk.

Amikor egy állomás kommunikál az Ethernet hálózaton, kereteket küld, amiben megtalálható a saját MAC-címe, mint forráscím és a kívánt célállomás MAC-címe. Bármelyik állomás, amelyik fogad egy keretet, dekódolja azt, majd kiolvassa a cél MAC-címet. Ha ez a cím egyezik a hálózati csatolóján konfiguválttal, akkor feldolgozza és továbbítja a megfelelő alkalmazás számára. Ha a cél MAC-cím nem egyezik meg az állomás MAC-címével, akkor a hálózati csatoló figyelmen kívül hagyja az üzenetet.

3.3.4 Ethernet kommunikáció

Az Ethernet protokoll szabványa a hálózati kommunikáció számos jellemzőjét meghatározza, úgy mint a keret formátumát, a keret méretét, az időzítést és a kódolást.

Amikor az Ethernet hálózaton az állomások üzeneteket küldenek egymásnak, akkor a szabványban meghatározott keretnek megfelelő szerkezetre formázzák az üzeneteket. A kereteket Protokoll Adat Egységeknek (PDUs - Protocol Data Units) is nevezik.

Az Ethernet keret formátumában meghatározott helye van a cél és a forrás MAC-címének, valamint az alábbi kiegészítő információknak:

- Szekvencia és időzítő előtag
- Kezdetjelző
- Keret hossz és típus
- Keret ellenőrző sorozat az átviteli hibák detektálásához

Az Ethernet keret mérete korlátozott: maximum 1528 bájt, minimum 64 bájt. A fogadóállomás nem dolgozza fel azokat a kereteket, amiknek a mérete nem fér bele ebbe az intervallumba. A keretformátumokon, a méreteken és az időzítéseken kívül az Ethernet szabvány definiálja, hogy a kereteket felépítő bitek hogyan legyenek kódolva a csatornára. A bitek a rézvezetéken elektromos impulzusok formájában, míg optikai kábelen fényimpulzusok formájában továbbítódnak.

Az Ethernet keret felépítése

Előtag	SFD	a cél MAC-címe	a forrás MAC címe	Hossz/típus	Beágyazott adat	Keretellenőrző összeg
7	1	6	6	2	46-tól 1500-ig	4

IEEE 802.3 Ethernet keret mezői

Bájtok	Mező név
7	Előtag
1	Keretkezdet
6	a cél MAC címe
6	a forrás MAC címe
2	Hossz/típus mező
46-tól 1500-ig	Beágyazott adat
4	Keretellenőrző összeg (CRC)

3.3.5 Ethernet hálózatok hierarchikus felépítése

Képzeljük el, hogy milyen nehéz lenne a kommunikáció, ha az egyetlen mód, hogy üzenetet küldjünk valakinek az lenne, hogy a személy nevét használjuk. Ha a címzésben nem használhatnánk utca-, város és ország nevet, szinte lehetetlen lenne üzenetet küldeni valakinek a nagyvilágban.

Az Ethernet hálózat egy állomásának MAC-címe a személynévhez hasonló. A MAC-cím egyértelműen azonosítja a címet viselő állomást, de semmit sem mond arról, hogy az állomás hol található a hálózaton. Ha az Internet összes állomását (több mint 4 millió) csupán az egyedi MAC-címük azonosítaná, akkor borzasztóan nehéz lenne bármelyiket is megtalálni közülük.

Az Ethernet technológia ráadásul nagy mennyiségű szórásos forgalmat generál az állomások kommunikációjához. A szórásos üzenetet az egy hálózatban lévő összes állomás megkapja. A szórásos üzenetek sávszélességet emésztenek fel, és lassítják a hálózat teljesítményét. Mi történne, ha az Internetre kapcsolt állomások milliói egy Ethernet hálózatban lennének, és szórásos üzeneteket használnának?

E két ok miatt a sok állomást tartalmazó nagy Ethernet hálózatok nem hatékonyak. Jobban megéri a nagy hálózatokat kisebb, jobban kezelhető részekre osztani. A nagy hálózatok felosztásának egyik módja a hierarchikus tervezési modell használata.

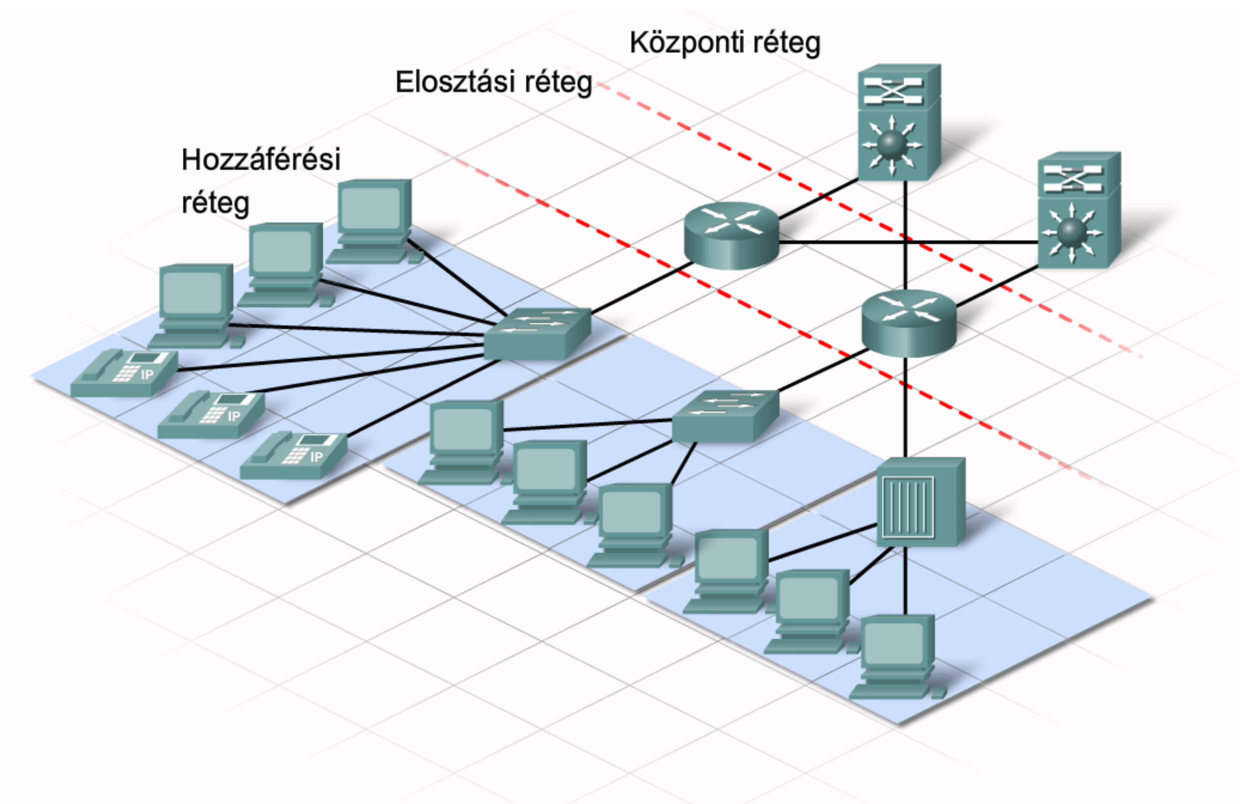
A hálózattervezés hierarchikusan rétegezett felépítésű csoportosítással szervezi az eszközöket egymásra épülő kisebb hálózatokba. Az így kialakított rendszer kisebb és jobban kezelhető eszközcsoportokból épül fel, ezáltal biztosítható, hogy a helyi forgalom helyi maradjon, és csak a más hálózatokba irányuló forgalom továbbítódjon a felsőbb rétegek felé.

A hierarchikusan rétegezett kialakítás biztosítja a hatékonyságot és a sebesség növekedését, a funkciók optimalizálását. Lehetővé teszi, hogy a hálózat igény szerint bővíthető legyen, vagyis további helyi hálózatokat adhatunk hozzá anélkül, hogy ez befolyásolná a meglévő teljesítményét.

A hierarchikus tervezésnek három alaprétege van:

- **Hozzáférési réteg** - a helyi Ethernet hálózaton az állomásoknak biztosít kapcsolódást.
- **Elosztási réteg** - kisebb helyi hálózatokat kapcsol össze.
- **Központi réteg** - nagy sebességű kapcsolat teremt az elosztási réteg eszközei között.

Ebben az új, hierarchikus tervezéssel létrehozott rendszerben olyan logikai címzési sémára van szükségünk, amivel azonosítani tudjuk az állomások helyét. Az Internet Protokoll (IP) címzési sémája megfelel ennek a célnak.



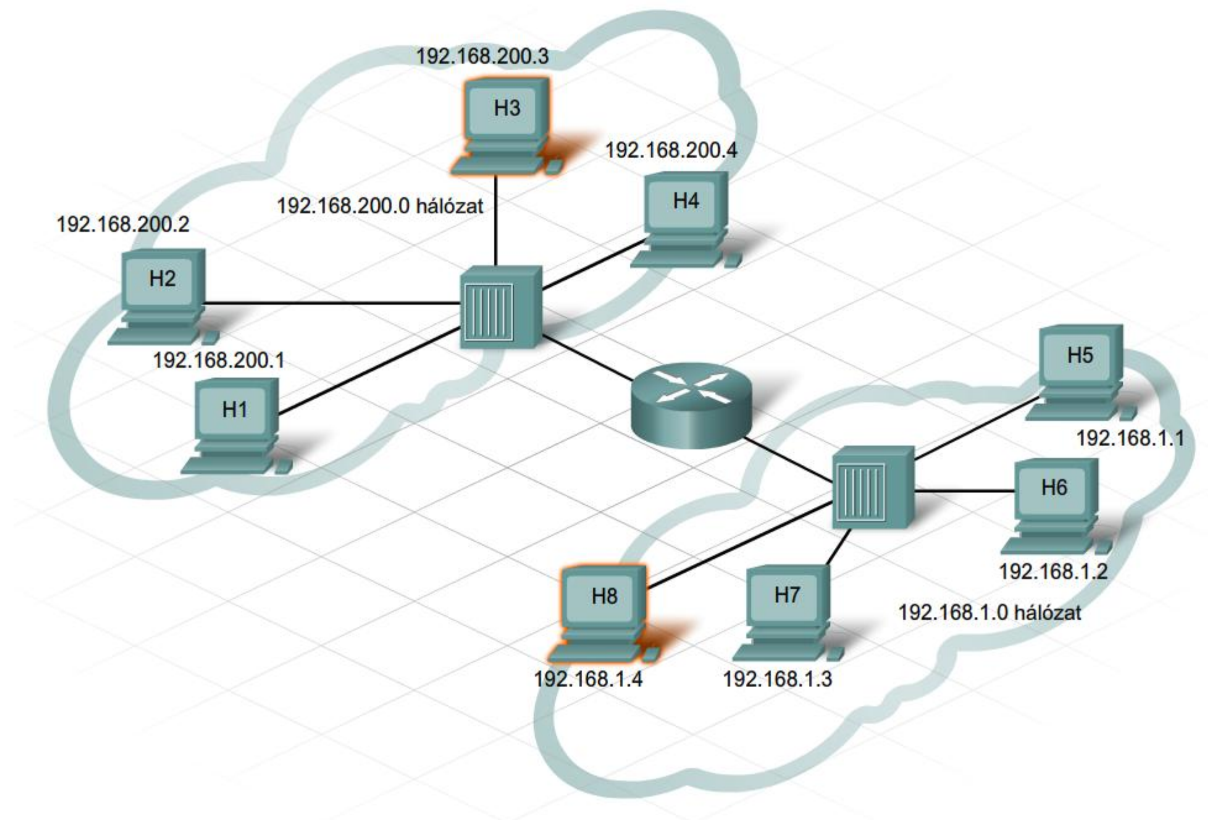
3.3.6 Logikai címzés

Egy személy neve általában nem változik, de a személy címe a lakóhelyéhez kötődik, és ezért változhat. Egy állomás esetén a fizikai címként is ismert MAC-cím nem változik; fizikailag hozzá van rendelve a hálózati csatolójához. A fizikai cím ugyanaz marad, függetlenül attól, hogy az állomás hol helyezkedik el a hálózaton belül.

Az IP-cím hasonló egy személy címéhez. Logikai címként ismert, mivel az állomás helye alapján logikailag van kijelölve. Az IP-címet (hálózati cím), a helyi hálózat címzéséhez illeszkedően a hálózati rendszergazda jelöli ki minden állomáshoz.

Az IP-cím két részből áll. Az egyik rész azonosítja a helyi hálózatot. Az IP-cím hálózati része megegyezik az összes, azonos hálózatban található állomásnál. Az IP-cím másik része azonosítja az állomást. Egy helyi hálózaton az IP-cím állomás része minden állomás esetén egyedi.

Hasonlóan, ahogy szükség van névre és címre ahhoz, hogy levelet küldjünk valakinek, úgy a fizikai MAC- és a logikai IP-cím is szükséges a számítógépek számára, hogy kommunikálni tudjanak egy hierarchikus hálózaton keresztül.



3.3.7 Hozzáférési és Elosztási rétegek és Eszközök

Az IP forgalom irányítása a hozzáférési, az elosztási és a központi réteghez rendelt eszközök és jellemzők alapján történik. Az IP címet annak eldöntésére használjuk, hogy a hálózati forgalmat helyben vagy a hálózat hierarchikus rétegein keresztül mozgatva kezeljük.

Hozzáférési réteg

A hozzáférési réteg minden végfelhasználói eszköz számára egy csatlakozási pontot biztosít, és lehetővé teszi több állomás számára, hogy hálózati eszközökön - rendszerint hubon vagy kapcsolón - keresztül kapcsolódjanak más állomásokhoz. A hozzáférési réteg egy elkülönített hálózatában jellemzően minden eszköz IP címének hálózati része azonos.

Ha az üzenetet a cél IP címének hálózati része szerint egy helyi állomásnak címezték akkor az üzenet helyi marad. Ha azonban a címzett más hálózatban helyezkedik el, akkor az üzenet az elosztási réteg felé továbbítódik. A hubok és a kapcsolók az elosztási rétegbeli eszközökhöz biztosítanak kapcsolatot. Az elosztási rétegben használt leggyakoribb eszköz a forgalomirányító.

Elosztási réteg

Az elosztási réteg csatlakozási pontot biztosít az elkülönített hálózatokhoz és szabályozza a hálózatok közötti információáramlást. Az elosztási rétegben találhatók a hozzáférési réteg kapcsolóinál nagyobb teljesítményű kapcsolók, csakúgy, mint a hálózatok közötti forgalomirányítást végző

forgalomirányítók . Az elosztási réteg eszközei szabályozzák a hozzáférési réteg irányából a központi réteg irányába folyó forgalom típusát és mennyiségét.

Központi réteg

A központi réteg egy nagysebességű gerinc, redundáns (tartalék) kapcsolatokkal. Ez a réteg több végfelhasználói hálózat közötti nagymennyiségű adat szállításáért felelős. A központi réteg elsődleges célja az adatok gyors szállítása.

A hubokat, a kapcsolókat és a forgalomirányítókat a következő két részben fogjuk részletesebben tárgyalni.

3.4 Egy Ethernet hálózatban a hozzáférési réteg (Acces Layer) építése

3.4.1 Hozzáférési réteg

A hozzáférési réteg a hálózat alapvető része, amelyben a felhasználók más állomásokhoz, megosztott fájlokhoz és nyomtatókhoz férnek hozzá. A hozzáférési réteg állomásokból és azok összekapcsolását biztosító hálózati eszközökből épül fel.

A hálózati eszközök lehetővé teszik számunkra, hogy több állomást kapcsoljunk össze, továbbá biztosítják a hálózaton keresztül elérhető szolgáltatásokhoz való hozzáférést. A kábellel közvetlenül összekötött, két állomásból álló egyszerű hálózatokkal ellentétben, a hozzáférési rétegben minden állomás egy hálózati eszközhöz csatlakozik. Ezt a csatlakozási típust mutatja az ábra.

Egy Ethernet hálózatban minden állomás egy kábel segítségével tud közvetlenül csatlakozni egy hozzáférési rétegbeli hálózati eszközhöz. Ezeket a kábeleket az Ethernet szabványoknak megfelelően gyártják. A kábel egyik végét az állomás hálózati csatolójához, míg a másikat a hálózati eszköz egy portjához kell csatlakoztatni. Többfajta olyan hálózati eszköz létezik, amit az állomások elérési réteghez történő csatlakoztatására használunk. A két legjellemzőbb ilyen eszköz a hub és a kapcsoló.

3.4.2 Hubok feladatai

A hub a hálózati eszközök egyik típusa, amely az Ethernet hálózatok hozzáférési rétegében helyezkedik el. A hub több porttal rendelkezik, ezeken keresztül állomásokat kapcsolhatunk a hálózathoz. A hubok egyszerű eszközök, nem rendelkeznek a hálózati állomások között küldött üzenetek dekódolásához szükséges elektronikával, nem képesek meghatározni, hogy melyik üzenetet melyik állomásnak kell megkapnia. A hub az egyik portján veszi az ektronikus jeleket, ezeket regenerálja és az összes többi portjára továbbítja.

Emlékezzünk rá, hogy egy állomás hálózati csatolója csak a saját MAC-címével címzett üzenetet fogadja. Az állomások figyelmen kívül hagyják a nem nekik szóló üzeneteket. Az üzenetet csak a célcímben megadott állomás dolgozza fel és válaszolja meg a küldőnek.

Az Ethernet hub összes portja egyetlen közös csatornán végzi az üzenetek küldését és fogadását. Mivel minden állomásnak osztoznia kell az elérhető csatorna sávszélességén, a hubra osztott-sávszélességű eszközként szoktak hivatkozni.



Az Ethernet hubon keresztül egyszerre csak egy üzenet küldhető. Előfordulhat, hogy a hubhoz kapcsolódó két vagy több állomás egyszerre próbál üzenetet küldeni. Ha ez bekövetkezik, az üzenetet hordozó elektronikus jel a hubon belül ütközik a többi üzenet jelével.

Az ütközés hatására az üzenetek sérülnek, és az állomások számára olvashatatlanná válnak. A hub nem dekódolja az üzenetet, így nem érzékeli ha az üzenet sérült, ezért ilyenkor is továbbítja azt az összes portján. Azt a területet, amelyhez tartozó állomások az ütközés következtében sérült üzenetet kaphatnak, ütközési tartománynak nevezzük.

Ütközés esetén az ütközési tartományon belül elhelyezkedő állomások képesek észlelni, hogy a beérkezett üzenet sérült. Ilyenkor mindegyik küldő állomás vár egy rövid ideig, majd megpróbálja újraküldeni az üzenetet. Amint egyre több állomást csatlakoztatunk az ütközés tartományhoz, úgy nő az ütközések esélye. Sok ütközés sok újraküldést okoz. A nagy mennyiségű újraküldés torlódást okozhat, és lelassíthatja a hálózati forgalmat. A fentiek miatt az ütközési tartományok méretét lehetőség szerint korlátozni kell.

3.4.3 A kapcsolók feladatai

Az Ethernet kapcsoló (switch) a hozzáférési rétegben használt eszköz. Csakúgy, mint a hub, a kapcsoló is több állomást tud a hálózathoz csatlakoztatni. A hub-bal ellentétben, a kapcsoló képes arra is, hogy csak egy meghatározott állomásnak továbbítson egy üzenetet. Amikor az állomás egy másik állomásnak a kapcsolón keresztül küld üzenetet, a kapcsoló fogadja és dekódolja a keretet, majd kiolvassa belőle a fizikai (MAC) címet.

A kapcsolók által használt tábla, melyet MAC-cím táblának hívnak, tartalmaz egy listát az aktív portokról és a hozzájuk csatlakoztatott állomások MAC-címéről. Amikor egyik állomás üzenetet küld a másiknak, a kapcsoló ellenőrzi, hogy a cél MAC-cím megtalálható-e a táblázatban. Ha igen, akkor egy áramkörnek nevezett átmeneti kapcsolatot épít fel a forrás- és a célport között. Az új áramkör egy dedikált csatornát biztosít, amin keresztül a két állomás kommunikálhat. A kapcsolóhoz csatlakozó többi állomás nem osztozik ennek a csatornának a sávszélességén, és nem kapja meg a nem neki címzett üzeneteket. Az állomások között minden egyes új párbeszédnél egy új áramkör épül fel. Ezek a különálló áramkörök lehetővé tesznek egyidejűleg több párbeszédet, anélkül, hogy ütközés történne.

Mi történik olyankor, ha a kapcsoló egy olyan keretet kap, melynek címzettje a MAC-cím táblában nem szereplő állomás? Ha a cél MAC-cím nincs benne a táblában, a kapcsoló nem rendelkezik az egyedi áramkör kialakításához szükséges információval. Amikor a kapcsoló nem tudja eldönteni, hogy merre található a célállomás, egy elárasztásnak nevezett eljárást alkalmaz, mellyel az összes csatlakozott állomásnak továbbítja a keretet. Mindegyik állomás összehasonlítja az üzenet cél MAC-címét a saját címével, és csak a megfelelő célcímmel rendelkező állomás dolgozza fel az üzenetet, és válaszol a küldőnek.

Hogyan kerül be egy új állomás címe a MAC-cím táblába? A kapcsoló az állomások között küldött összes kereteket megvizsgálva építi fel a MAC-cím táblát. Amikor egy új állomás küld üzenetet, vagy egy elárasztásos üzenetre válaszol, a kapcsoló azonnal megtanulja az állomás MAC-címét és azt a portot amelyhez az állomás csatlakozik. A tábla dinamikusan frissül, minden alkalommal amikor új forrás MAC-című keret érkezik be, így a kapcsoló gyorsan megtanulja az összes hozzá csatlakoztatott állomás MAC-címét.

Néha szükség lehet arra, hogy a kapcsoló egyik portjához egy másik hálózati eszközt, például hub-ot csatlakoztassunk, így növelve meg a hálózathoz kapcsolható állomások számát. Amikor a kapcsoló egy portjához hub-ot csatlakoztatunk, a kapcsoló ahhoz a porthoz rendeli a hub-hoz csatlakoztatott összes állomás MAC-címét. Esetenként ugyanahhoz a hub-hoz tartozó két állomás akar kommunikálni. Ebben az esetben a kapcsoló fogadja a keretet, és a tábla alapján megállapítja, hogy a célállomás hol helyezkedik el. Ha mind a forrás, mind pedig a célállomás azonos porton található, a kapcsoló figyelmen kívül hagyja az üzenetet.

Amikor a kapcsoló portjához egy hub csatlakozik, ütközés történhet a hubon. A hub továbbítja az összes portjára az ütközés következtében sérült üzenetet. A kapcsoló fogadja ezt, de a hub-bal ellentétben nem továbbítja az ütközés következtében megsérült üzeneteket. Összességében a kapcsolónak megvan az a pozitív tulajdonsága, hogy minden portja különálló ütközési tartományt hoz létre. Minél kevesebb állomás van az ütközési tartományban, annál kisebb az esélye annak, hogy ütközés következik be.

3.4.4 Szórásos üzenetküldés

Ha az állomásokat hubon vagy kapcsolón keresztül kötjük össze, egy helyi hálózat jön létre. A helyi hálózaton belül gyakran szükséges, hogy egy állomás az összes többi állomásnak egyszerre tudjon üzenetet küldeni. Azt az üzenettípust, amivel ez megvalósítható, szórásnak (broadcast) nevezzük. A szórásos üzenet hasznos, ha egy állomás úgy próbál információt szerezni, hogy nem tudja a választ birtokló állomás címét, vagy amikor egy állomás egyszerre akarja eljuttatni ugyanazt az információt a hálózat összes többi állomásához.

Egy üzenet csak egy cél MAC-címet tartalmazhat. Vajon hogyan lehetséges egy állomás számára, hogy a helyi hálózaton belül kapcsolatba lépjen mindegyik állomással, anélkül, hogy mindegyiknek külön üzenetet küldene az egyedi MAC-címeket használva?

A probléma megoldásához a szórásos üzeneteket egy minden állomás által sajátjaként felismert egyedi MAC-címre küldik. A szórásos fizikai cím valójában egy 48-bites cím, amely csak egyesből áll. A hosszuk miatt a MAC-címeket általában hexadecimális jelöléssel ábrázoljuk. A szórásos üzenet hexadecimális jelölése: FFFF.FFFF.FFFF. Mindegyik hexadecimális F négy darab bináris egyest jelöl.

Amikor egy állomás egy szórási címre küldött üzenetet kap, fogadja azt, és úgy dolgozza fel, mintha közvetlenül neki címezték volna. Amikor egy állomás szórásos üzenetet küld, a hubok és kapcsolók továbbítják az üzenetet az azonos hálózatba tartozó minden állomásnak. Ebből a viselkedésből kifolyólag a helyi hálózatot szórási tartománynak is szokták nevezni.

Ha túl sok állomás csatlakozik egyazon szórási tartományhoz, a szórásos forgalom mértéke túlságosan is megnövekedhet. A helyi hálózat által kiszolgált állomások számát és a hálózati forgalmat korlátozzák az összekapcsolás során használt hubok és kapcsolók képességei. Újabb állomások hozzáadásával a hálózat növekszik, ami egyre nagyobb hálózati- és ezzel együtt szórásos forgalmat is jelenthet. A teljesítmény javítása érdekében gyakran szükség van egy helyi hálózatot vagy szórási tartományt több hálózatra bontani.

3.4.6 MAC és IP

Egy helyi Ethernet hálózatban a hálózati csatoló csak akkor fogadja a keretet, ha annak célcíme megegyezik a szórásos MAC-címmel vagy a csatoló saját MAC-címével.



A legtöbb hálózati alkalmazás azonban logikai IP-címet használ a kiszolgálók és ügyfelek helyének meghatározásához.

Mi van akkor, ha a küldő állomás a célállomásnak csak a logikai IP-címét ismeri? Hogyan határozza meg a küldő állomás, hogy melyik MAC-címet kell a keretbe helyeznie?

A küldő állomás egy címfeloldó protokollnak (ARP – Address Resolution Protocol) nevezett IP protokollt használhat annak érdekében, hogy kiderítse az azonos hálózatban található célállomás MAC-címét.

3.4.7 Címmeghatározó protokoll (ARP)

Ha egy állomásnak csak az IP címe ismert, az ARP egy három lépésből álló folyamattal deríti ki és tárolja le az állomás MAC-címét.

1. A küldő állomás létrehoz és elküld egy keretet a szórásos fizikai címre. A keret egy speciális üzenet mellett tartalmazza a célállomás IP-címét.

2. A hálózatban található összes állomás megkapja a szórásos keretet, és összehasonlítja az üzenetben található IP-címet a saját IP-címével. Az az állomás, ami egyezést talál, visszaküldi a MAC-címét az ARP-kérést megfogalmazó állomásnak.

3. A küldő állomás megkapja a válaszüzenetet, és az ARP-táblának nevezett táblázatban eltárolja az összetartozó MAC- és IP-címet.

Ha a küldő állomás ARP-táblájában szerepel a célállomás MAC-címe, akkor ARP-kérés nélkül, közvetlenül is tud a célállomásnak kereteket küldeni.

3.5 A hálózat Elosztási rétegének építése

3.5.1 Elosztási réteg

Ahogy növekszik a hálózat, gyakran szükséges, hogy egy helyi hálózatot több hozzáférési rétegbeli hálózatra bontsunk. Egyebek mellett az alábbi szempontok alapján oszthatunk fel egy hálózatot több részre:

- Fizikai elhelyezkedés
- Logikai funkció
- Biztonságra vonatkozó követelmények
- Alkalmazásokra vonatkozó követelmények

Az elosztási réteg összekapcsolja a hozzáférési réteg független helyi hálózatait, és szabályozza a köztük zajló forgalmat. Ez a réteg a felelős azért, hogy az azonos hálózaton belüli állomások közötti forgalom megmaradjon helyi forgalomnak, mivel csak a más hálózatokba címzett forgalmat továbbítja. Az elosztási réteg egyaránt szűrheti a bejövő és a kimenő forgalmat biztonsági és forgalom-szabályozási célból.

Az elosztási rétegbe tartozó eszközöket hálózatok, és nem egyéni állomások összekapcsolására tervezték. Az egyéni állomások hozzáférési rétegbeli eszközökkel, például hubok vagy kapcsolók



segítségével csatlakoznak a hálózathoz. A hozzáférési rétegbeli eszközök elosztási rétegbeli eszközökkel, például forgalomirányítókkal, vannak egymáshoz kapcsolva.

3.5.2 A forgalomirányítók feladatai

A forgalomirányító olyan hálózati eszköz, amely egy helyi hálózatot más helyi hálózatokhoz kapcsol. Az elosztási rétegben a forgalomirányítók irányítják a forgalmat, és a hatékony hálózati működéshez szükséges egyéb feladatokat is végrehajtanak. A forgalomirányítók, a kapcsolókhoz hasonlóan, dekódolják és elolvassák az általuk vett üzenetet. A kapcsolókkal ellentétben azonban, melyek csak a MAC-címet tartalmazó keretet értelmezik, a forgalomirányítók dekódolják a keretekbe beágyazott csomagokat is.

A csomagformátum tartalmazza a küldő- és forrásállomás IP-címét, valamint az adatüzenetet. A forgalomirányító kiolvassa a cél IP-cím hálózati részét, és ezt felhasználva keresi meg a csatlakoztatott hálózatok közül azt, amelyiken keresztül a legjobb út vezet a célhoz.

Minden esetben, amikor a forrás- és a célállomás IP-címének hálózati része nem egyezik meg, az üzenet továbbításához forgalomirányítót kell használni. Ha egy állomásnak, mely az 1.1.1.0 hálózatban található, üzenetet kell küldenie az 5.5.5.0 hálózatban található állomásnak, a küldő először a forgalomirányítónak továbbítja az üzenetet. A forgalomirányító fogadja azt, majd a cél IP-címének kiolvasásához kicsomagolja. Ezt követően eldönti, hogy merre továbbítsa az üzenetet, majd újra beágyazza a csomagot egy keretbe, és továbbítja a cél irányába.

Hogyan határozza meg a forgalomirányító, hogy melyik úton küldje az üzenetet, hogy az eljusson a célhálózatba?

A forgalomirányító mindegyik portja (interfésze) különböző helyi hálózathoz csatlakozik. Minden forgalomirányító tartalmaz egy táblát az összes közvetlenül csatlakoztatott hálózatról és az interfészekről, melyekkel csatlakoznak ezekhez a hálózatokhoz. Ezek az irányítótáblák tartalmazhatnak még információt olyan útvonalakról is, melyeket a forgalomirányító nem helyileg csatlakoztatott, távoli hálózatok eléréséhez használ.

Amikor a forgalomirányító egy keretet kap, dekódolja azt, hogy megvizsgálhassa a cél IP-címet tartalmazó csomagot. A forgalomirányító összehasonlítja a cél címet és az irányítótáblában található hálózatcímeket. Ha a célhálózat címe szerepel az irányítótáblában, a forgalomirányító a továbbküldéshez beágyazza a csomagot egy új keretbe, majd továbbítja azt a célhálózat felé vezető interfészen. A keretek célhálózat felé történő továbbításának folyamatát forgalomirányításnak nevezzük.

A forgalomirányító interfészei nem továbbítják azokat az üzeneteket, melyek célcíme szórásos fizikai cím. Ennek eredményeként a helyi hálózatok szórásos üzenetei nem jutnak át másik helyi hálózatba a forgalomirányítón keresztül.

3.5.3 Alapértelmezett átjáró

Hogyan határozza meg a forgalomirányító, hogy melyik úton küldje az üzenetet, hogy az eljusson a célhálózatba?

A forgalomirányító mindegyik portja (interfésze) különböző helyi hálózathoz csatlakozik. Minden forgalomirányító tartalmaz egy táblát az összes közvetlenül csatlakoztatott hálózatról és az



interfészekről, melyekkel csatlakoznak ezekhez a hálózatokhoz. Ezek az irányítótáblák tartalmazhatnak még információt olyan útvonalakról is, melyeket a forgalomirányító nem helyileg csatlakoztatott, távoli hálózatok eléréséhez használ.

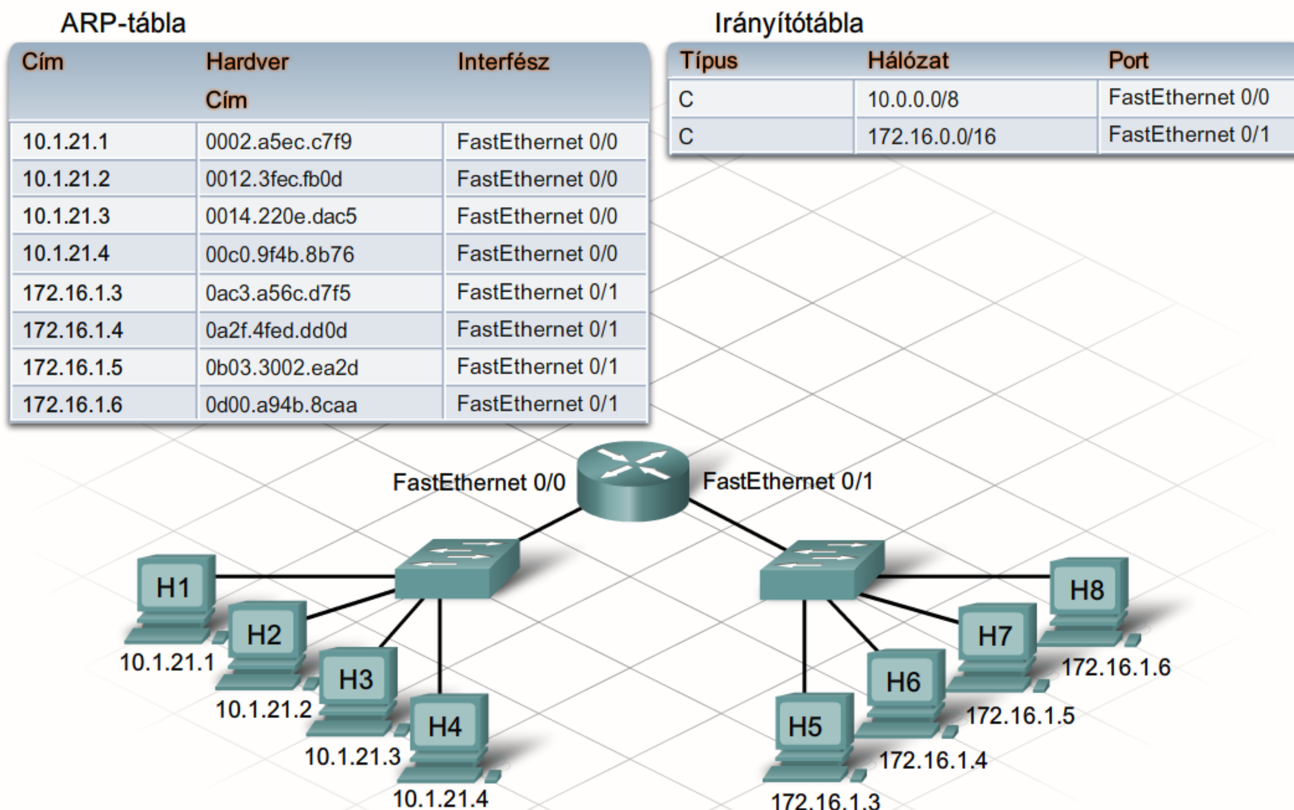
Amikor a forgalomirányító egy keretet kap, dekódolja azt, hogy megvizsgálhassa a cél IP-címet tartalmazó csomagot. A forgalomirányító összehasonlítja a cél címet és az irányítótáblában található hálózatcímeket. Ha a célhálózat címe szerepel az irányítótáblában, a forgalomirányító a továbbküldéshez beágyazza a csomagot egy új keretbe, majd továbbítja azt a célhálózat felé vezető interfészen. A keretek célhálózat felé történő továbbításának folyamatát forgalomirányításnak nevezzük.

A forgalomirányító interfészei nem továbbítják azokat az üzeneteket, melyek célcíme szórásos fizikai cím. Ennek eredményeként a helyi hálózatok szórásos üzenetei nem jutnak át másik helyi hálózatba a forgalomirányítón keresztül.

3.5.4 A forgalomirányítók által karbantartott táblák

A forgalomirányítók a helyi és a távoli hálózatok között mozgatják az információt. Ehhez, mind az ARP-, mind pedig az irányítótáblákban tárolt információt használniuk kell. Az irányítótáblák nem foglalkoznak az állomások egyedi címeivel, csupán a hálózatok címeit és a hozzájuk vezető legjobb utat tartalmazzák. Az irányítótáblák bejegyzései kétféleképpen keletkezhetnek: a hálózatban található más forgalomirányítók információi alapján dinamikusan frissülnek, vagy a hálózati rendszergazda írja be őket kézzel. A forgalomirányítók az irányítótáblájukat használják annak eldöntésére, hogy melyik interfészen kell továbbítani az üzenetet, hogy az elérje a célját.

Ha a forgalomirányító nem tudja meghatározni, hogy merre küldje az üzenetet, akkor eldobja azt. A hálózati rendszergazdák egy alapértelmezett útvonalat állíthatnak be annak érdekében, hogy az irányítótáblában nem szereplő célcímek esetén a forgalomirányító ne dobja el a csomagot. Az alapértelmezett útvonal az az interfész, melyen keresztül a forgalomirányító az ismeretlen cél IP-hálózati címet tartalmazó csomagokat továbbítja. Az alapértelmezett útvonal általában egy másik forgalomirányítóhoz csatlakozik, amely képes a csomagot annak célhálózata felé továbbítani.



ARP-tábla

Cím	Hardver Cím	Interfész
10.1.21.1	0002.a5ec.c7f9	FastEthernet 0/0
10.1.21.2	0012.3fec.fb0d	FastEthernet 0/0
10.1.21.3	0014.220e.dac5	FastEthernet 0/0
10.1.21.4	00c0.9f4b.8b76	FastEthernet 0/0
172.16.1.3	0ac3.a56c.d7f5	FastEthernet 0/1
172.16.1.4	0a2f.4fed.dd0d	FastEthernet 0/1
172.16.1.5	0b03.3002.ea2d	FastEthernet 0/1
172.16.1.6	0d00.a94b.8caa	FastEthernet 0/1

Irányítótábla

Típus	Hálózat	Port
C	10.0.0.0/8	FastEthernet 0/0
C	172.16.0.0/16	FastEthernet 0/1

Egy forgalomirányító a következő két helyre továbbíthat kereteket: a célállomást tartalmazó közvetlenül csatlakoztatott hálózatba, vagy a célállomáshoz vezető útvonalon szereplő másik forgalomirányítóhoz. Mielőtt a forgalomirányító az Ethernet interfészén keresztül továbbítaná az üzenetet, létre kell hoznia a keretet, amiben el kell helyeznie a cél MAC-címet.

Abban az esetben, ha a célállomás a forgalomirányítóhoz csatlakoztatott helyi hálózatban található, a fenti cím a célállomás MAC-címe. Ha azonban egy másik forgalomirányítónak kell továbbítani a keretet, akkor ennek a szomszédos forgalomirányítónak a MAC-címe kerül a keretbe. A forgalomirányítók az ARP táblájuk alapján határozzák meg ezeket a címeket.

A forgalomirányító mindegyik interfésze tagja annak a helyi hálózatnak, amelyhez csatlakoztatva van, és mindegyik ilyen hálózathoz saját ARP táblát tart fent. Az ARP tábla tartalmazza a hálózatban található összes egyedi állomás MAC- és IP-címét.

3.5.5 Helyi számítógép hálózat(LAN)

A helyi hálózat (LAN - Local Area Network) kifejezés vagy egy önálló helyi hálózatra utal, vagy egy csoport, közös adminisztratív irányítás alatt álló, egymással összekötött helyi hálózatra. A hálózatok kezdeti időszakában a helyi hálózatokat fizikailag egy területen elhelyezkedő, kisméretű hálózatként határozták meg. Amíg helyi hálózatnak tekintjük az egyszerű otthoni vagy kisebb irodai hálózatokat, addig a több száz állomást tartalmazó, egymással összekötött, több épületet és helyet magában foglaló helyi hálózatokra is kiterjed a LAN fogalma.

Fontos szem előtt tartani, hogy minden helyi hálózat azonos adminisztratív irányítás alatt áll. A helyi hálózatok másik közös tulajdonsága, hogy jellemzően Ethernet vagy vezeték nélküli protokollokat használnak, és nagy átviteli sebesség jellemzi őket.

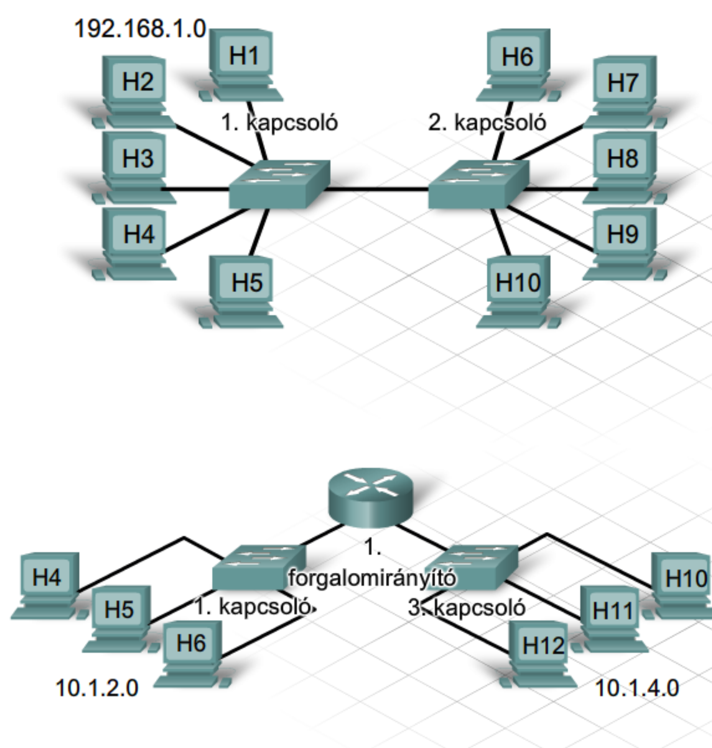
Az Intranet kifejezés gyakran egy szervezethez tartozó privát LAN-t jelöl, amit úgy terveztek, hogy csak a szervezet tagjai, alkalmazottai vagy más felhatalmazással rendelkezők férhessenek hozzá.

3.5.6 Állomások felvétele, helyi és távoli hálózatokba

A LAN-on belül az összes állomást elhelyezhetjük egyetlen helyi hálózatba, de szét is oszthatjuk őket több, az elosztási réteggel összekapcsolt hálózatba. A megfelelő eljárás az elvárt eredménytől függ. Ha az állomásokat egyetlen helyi hálózatba tesszük, lehetővé válik, hogy mindenki közvetlenül kommunikálhasson egymással. Ebben az esetben csak egy szórási tartomány van, és az állomások ARP protokollt tudnak használni egymás megkereséséhez.

Egy egyszerű hálózati tervben előnyös lehet minden állomást egyetlen helyi hálózatba tenni. Ahogy a hálózat növekszik, a megnövekedett forgalom lecsökkenti a hálózat teljesítményét és sebességét. Ebben az esetben szükségszerű lehet az állomások egy részét egy másik hálózatba áthelyezni.

Ha az új hálózatba további állomásokat helyezünk ennek az eredeti hálózat forgalmára gyakorolt hatása csökkeni fog. Ugyanakkor az egyik hálózatban található állomás forgalomirányító nélkül már nem fog tudni kommunikálni a másik hálózatban található állomásokkal. A forgalomirányítók bonyolultabbá teszik a hálózati konfigurációt, és késleltetést eredményeznek a helyi hálózatból egy másik hálózatba küldött csomag továbbításában.



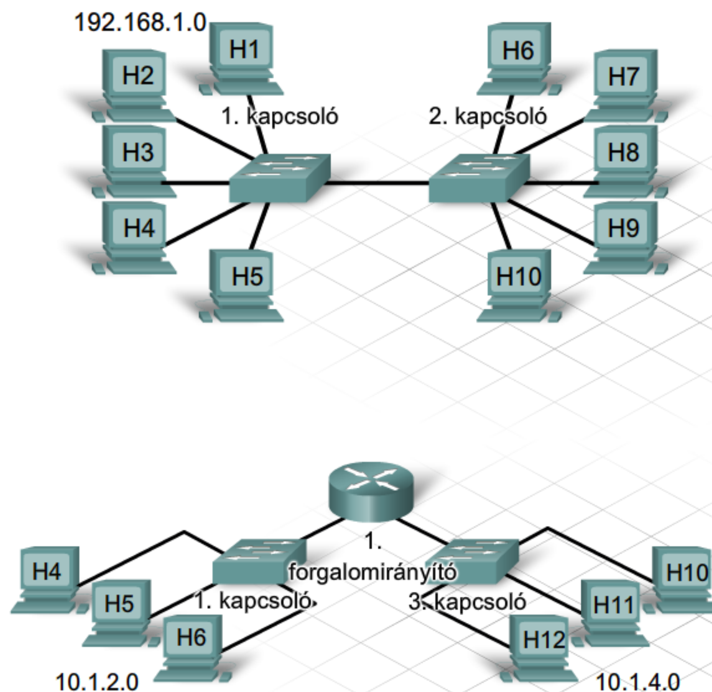
Az összes állomás egyetlen helyi hálózati szegmensre helyezése

Előnyök:

- Egyszerű hálózatokban megfelelő
- Kisebb bonyolultság és alacsonyabb hálózati költség
- Annak engedélyezése, hogy az állomások "lássák" egymást.
- Gyorsabb adatátvitel - közvetlenebb kommunikáció
- Könyebb eszköz hozzáférés

Hátrányok:

- Minden állomás egyetlen üzenetszórási tartomány része, ami nagyobb forgalmat és kisebb teljesítményt eredményez a szegmensen



A LAN topológiákra kattintva az egyszerű illetve összetett helyi hálózatok fenntartásának előnyei és hátrányai láthatók.

Az állomások távoli hálózati szegmensre helyezése

Előnyök:

- Alkalmasabb a nagyobb és összetettebb hálózatokban
- Felosztja az üzenetszórási tartományokat és csökkenti a forgalmat
- Minden szegmensen növeli a teljesítményt
- Más, helyi hálózati szegmensen lévő állomások számára az eszközök láthatatlanok lesznek
- Növeli a hálózati biztonságot
- Megkönnyíti a hálózat szervezését

Hátrányok:

- Forgalomirányítás szükséges (elosztási réteg)
- A forgalomirányító lassítja a szegmensek közötti forgalmat
- Bonyolultabb és költségesebb (forgalomirányítót igényel)

3.6 Egy helyi hálózat tervezése és csatlakoztatása

3.61. Tervezz meg és dokumentálj egy Ethernet hálózatot

A legtöbb helyi hálózat Ethernet technológián alapul. Ez a technológia gyors és hatékony ha megfelelően tervezett és összeállított hálózatban használják. A jó hálózat megvalósításának kulcsa a hálózat megépítését megelőző tervezés.

Egy hálózat tervezése a hálózat használatára vonatkozó információk gyűjtésével kezdődik. Ez a következőket jelenti:

- A hálózathoz csatlakoztatandó állomások száma és típusa
- A használandó alkalmazások
- Megosztási és Internet kapcsolat követelményei
- Biztonsági és titoktartási megfontolások
- Megbízhatósági és rendelkezésre állási elvárások
- Vezetékes és vezeték nélküli kapcsolódási követelmények

A hálózat telepítésének tervezése során számos tényezőt kell figyelembe venni. Mielőtt a hálózati eszközöket megvásárolnánk és csatlakoztatnánk az állomásokat, meg kell tervezni és dokumentálni kell a hálózat logikai és fizikai topológiai térképét. Néhány szempont, amit érdemes megfontolni:

A telepítendő hálózat fizikai környezete:



- Hőmérsékletszabályzás (a megfelelő működés érdekében minden eszköznek egy meghatározott hőmérsékletet és páratartalmat kell biztosítani)
- Hozzáférhetőség és az áramforrás elhelyezkedése

A hálózat fizikai kiépítése:

- Az eszközök (forgalomirányítók, kapcsolók, állomások) fizikai elhelyezkedése
- Az eszközök csatlakoztatásának módja
- A kábelek helye és elhelyezkedése
- A végberendezések (állomások, kiszolgálók) hardverbeállítása

A hálózat logikai konfigurációja:

- A szórási és ütközési tartományok helye és mérete
- IP-címzési séma
- Elnevezési séma
- Megosztási beállítások
- Jogok

3.6.2 Prototípusok

Az állomások száma és típusa - Hol vannak a végfelhasználók? Milyen típusú hardvert használnak? Hol vannak a kiszolgálók, a nyomtatók és a többi hálózati eszközök?

Alkalmazások - Milyen alkalmazásokat futtatnak a hálózaton?

Megosztandó adatok és eszközök - Ki akar hozzáférni fájlhoz és hálózati erőforrásokhoz, például nyomtatókhoz?

Sávszélesség követelmények (sebesség) - Mi az elfogadható sebesség a végfelhasználók számára? Az összes felhasználó igényli ezt a áteresztőképességet? Milyen hatása van az alkalmazásoknak az áteresztőképességre?

Biztonság - A hálózaton mozgatott adat személyes vagy érzékeny jellegű? Ezen információkhoz való jogosulatlan hozzáférés káros lehet valakire?

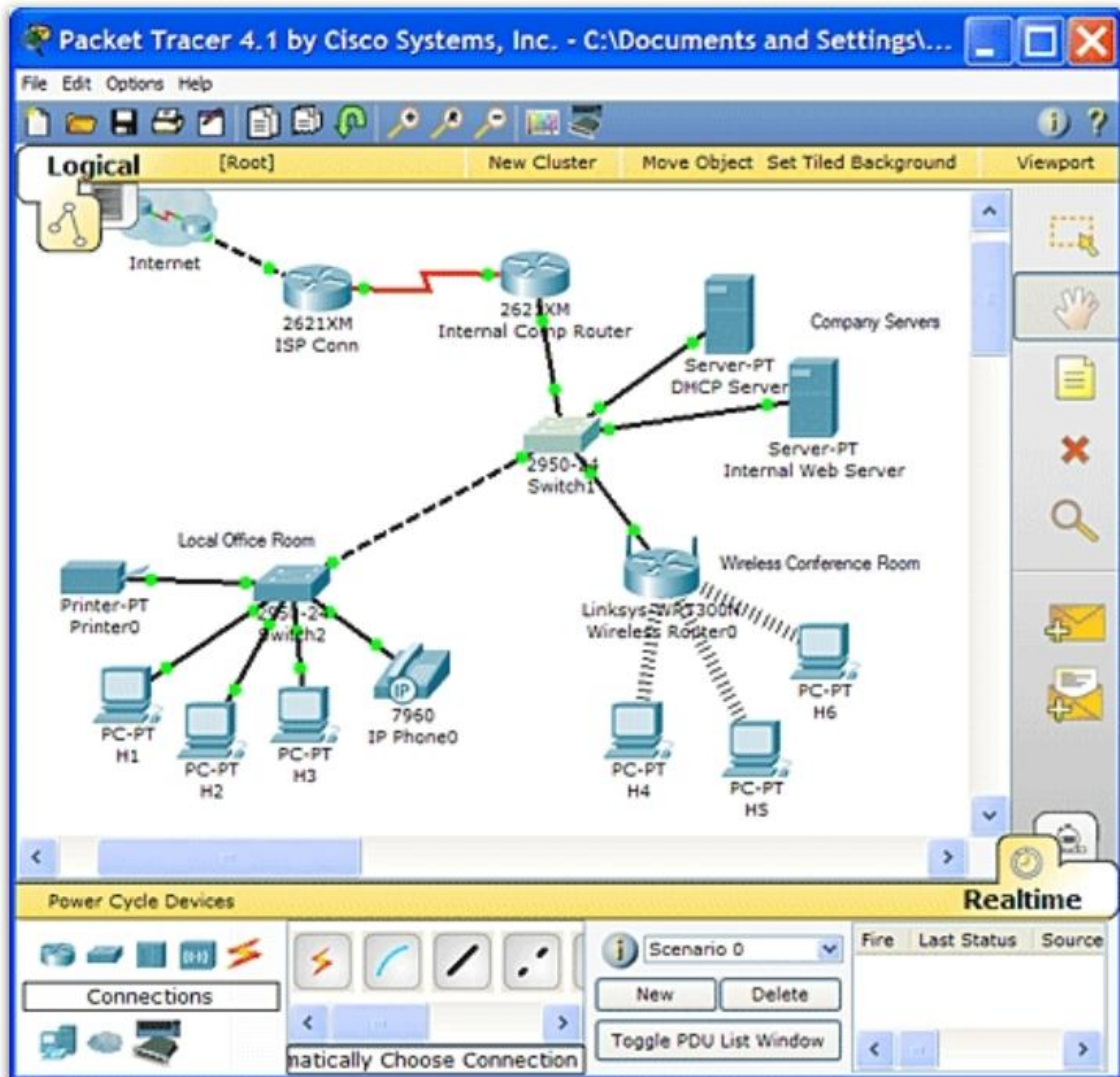
Megbízhatóság - Milyen fontos a hálózat? Szükséges a 100%-os rendelkezésre állás? (ez működési időként ismert) Mennyi leállási idő tolerált?

Követelmények a vezeték nélküli hálózathoz - Egy vagy minden végfelhasználó igényel vezeték nélküli kapcsolatot?

Miután a hálózati követelményeket dokumentáltuk, és elkészült a fizikai és logikai topológiai térkép is, a végrehajtási folyamat következő lépése a hálózati terv tesztelése. A hálózati terv tesztelésének egyik módja, hogy a hálózatról készítünk egy működő modellt vagy prototípust.

A prototípuskészítés elengedhetetlenné válik, amint a hálózat növekszik és egyre bonyolultabb lesz. A prototípus megmutatja a hálózati rendszergazda számára, hogy a tervezett hálózat a vártnak megfelelően működik-e, még mielőtt az eszközökre és az üzembe helyezésükre pénzt költenénk. A dokumentációnak a prototípuskészítés folyamatának minden szempontját magában kell foglalnia.

Különböző eszközök és technikák állnak rendelkezésre a hálózati prototípus készítéséhez; köztük a valódi eszközök laborkörnyezetben történő összeállításának lehetősége, vagy a modellező és szimulációs eszközök használata. A Packet Tracer példaként szolgál a prototípus készítéséhez használható szimulációs és modellező eszközre.



3.6.3 Multi funkciós eszköz

A legtöbb otthoni és kisebb irodai hálózatban nincs szükség az üzleti környezetben használt nagy teljesítményű eszközökre. Ebben a helyzetben ugyan a kisebb tudású eszközök is megfelelhetnek, ugyanakkor forgalomirányítási és kapcsolási funkciókra ugyanúgy szükség lehet, mint a nagy hálózatoknál. Ez a szükséglet több hálózati eszköz funkcióját magába foglaló eszközök kifejlesztéséhez vezetett. Ilyen eszköz például az a forgalomirányító, amely rendelkezik kapcsoló és vezeték nélküli hozzáférési pont funkciókkal is. A tananyag további részében ezekre a multifunkciós eszközökre integrált forgalomirányítókként fogunk hivatkozni. Az integrált forgalomirányítók skálája az otthoni és kisebb üzleti felhasználásra tervezett eszközöktől egészen a komolyabb teljesítményű, nagyobb vállalati fiókokat is kiszolgáló eszközökig terjedhet.

Az integrált forgalomirányító olyan, mintha számos különböző eszközt kapcsolnánk egymáshoz. Az eszközben működő kapcsoló és forgalomirányító között például összeköttetés van, de ez a kapcsolat az eszközön belül valósul meg. Amikor egy szórásos üzenet érkezik a kapcsoló egy portjára, az integrált forgalomirányító továbbítja a szórásos üzenetet minden kapcsolóportra, beleértve a belső forgalomirányító csatlakozást is. A forgalomirányító részegység megakadályozza a szórásos üzenet továbbhaladását.

Az otthoni és kisebb irodai hálózatok számára léteznek olcsó multifunkciós eszközök, melyek integrált forgalomirányítást, kapcsolást, vezeték nélküli és biztonsági lehetőségeket kínálnak. Egy ilyen integrált forgalomirányító típusra példa a Linksys vezeték nélküli forgalomirányító. Ez az eszköz egyszerűen tervezett és az alkotóelemek jellemzően nem különülnek el. Meghibásodás esetén nem lehetséges az elromlott egység kicserélése. Ezek az eszközök, mint integrált forgalomirányítók nem egy funkcióra lettek optimalizálva, esetleges meghibásodásuk az eszköz összes funkcióját érinti.

Az integrált forgalomirányítókra egy másik példa a Cisco integrált szolgáltatási forgalomirányító vagy más néven ISR. A Cisco ISR termékcsalád széles palettán kínál termékeket, ideértve a kisebb irodai és otthoni irodai környezetbe tervezett eszközöket, csakúgy mint a nagyobb hálózatokba szánt berendezéseket. Számos ISR kínál modularitást. Ezekben a típusokban minden funkció (kapcsoló, forgalomirányító stb.) különálló komponensből áll, ami lehetővé teszi az igényekhez illeszkedő egyedi komponensek hozzáadását, kicserélését és fejlesztését.

3.6.4 Linksys forgalomirányító csatlakoztatás

Egy kapcsoló portjaihoz csatlakoztatott összes eszköznek ugyanabban a szórási tartományban kell lennie. Ez azt jelenti, hogy minden ilyen eszköz IP-címének azonos hálózatba kell tartoznia. Az olyan eszközök, melyek IP-címének hálózati része eltérő, nem fognak tudni kommunikálni a többi eszközzel.

A Microsoft Windows operációs rendszerei számítógép-neveket használnak az eszközök azonosítására a hálózaton. Ezeket a neveket, csakúgy mint az IP-címeket, érdemes szerepeltetni a tervezési dokumentációban, hiszen ezzel megkönnyíthetjük a jövőbeli hibaelhárítást.

A Microsoft Windows aktuális IP beállításának megjelenítéséhez használjuk az ipconfig parancsot. Részletesebb információ, beleértve az állomás nevet is, az ipconfig /all paranccsal érhető el. Dokumentáljunk minden információt a kapcsolatról és a beállítási folyamatról!

Miután az állomások már kommunikálnak a hálózaton, dokumentálni kell a hálózati teljesítményre vonatkozó adatokat is. A normális működés során végzett teljesítményadatok rögzítését hálózati alapszint meghatározásnak hívják. Amikor később a hálózat teljesítményét összehasonlítjuk a viszonyítási ponttal, az eltérések rávilágíthatnak a lehetséges problémákra.

3.6.5 Erőforrás megosztás

A hálózatok egyik leggyakoribb célja az olyan jellegű erőforrások megosztása, mint a fájlok és a nyomtatók. A Windows XP lehetővé teszi távoli felhasználók számára, hogy a megosztási funkción keresztül hozzáférjenek a helyi géphez és annak erőforrásaihoz. Érdemes az ezzel kapcsolatos biztonsági kérdéseket átgondolni, és a megosztott erőforrásokhoz a jogosultságot körültekintően szabályozni.

Alapértelmezetten a Windows XP egy egyszerű fájlmegosztás néven ismert folyamatot használ. Egyszerű fájlmegosztással nem akadályozhatjuk meg, hogy a megosztott fájlokat adott felhasználók és csoportok ne érjék el.

Az egyszerű fájlmegosztás kikapcsolható, így sokkal specifikusabb biztonsági hozzáférési szintet állíthatunk be. Amikor ezt elvégeztük, a következő jogokat lehet az erőforrásokhoz rendelni:

- Teljes hozzáférés
- Módosítás
- Olvasás és végrehajtás
- Mappa tartalmának listázása
- Olvasás
- Írás

Amikor egy felhasználó hozzáfér egy távoli eszközön levő fájlokhoz, a Windows Explorer lehetővé teszi a felhasználó számára, hogy egy meghajtót rendeljen a távoli könyvtárhoz vagy erőforráshoz. Ez az eljárás egy adott meghajtó-betűjelet (például M:), rendel a távoli erőforráshoz, ami lehetővé teszi a felhasználó számára, hogy az erőforrást úgy kezelje, mintha az helyben lenne csatlakoztatva.

3.7 A fejezet összefoglalása

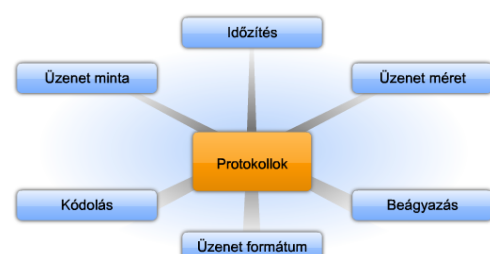
3.7.1 Összegzés

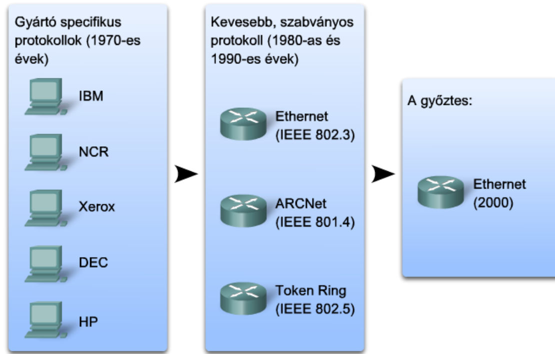


Ez a fejezet az alapvető fogalmakkal, a hálózatok előnyeivel, és a helyi Ethernet hálózatok jellemzőivel foglalkozik.

- Az információs hálózatok hangot, videót és adatot tudnak szállítani.
- Az információs hálózatok perifériákból, állomásokból, hálózati eszközökből és átviteli közegekből állnak.
- A topológiai ábrákat a logikai és a fizika hálózattervek leírására használjuk.
- Az állomások lehetnek kliensek, kiszolgálok vagy mind a kettő.

- Minden kommunikációnak van forrása, célja és csatornája.
- A számítógépes kommunikációk speciális szabályok alapján működnek, ezeket hívják protokolloknak.
- A protokollok definiálják az üzenet jellemzőit, mint: kódolás, formázás, beágyazás, méret, időzítés és minták.



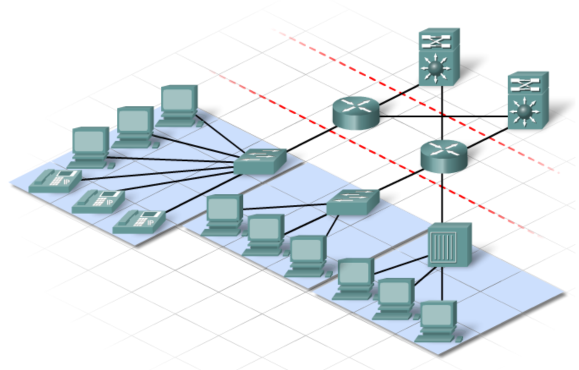


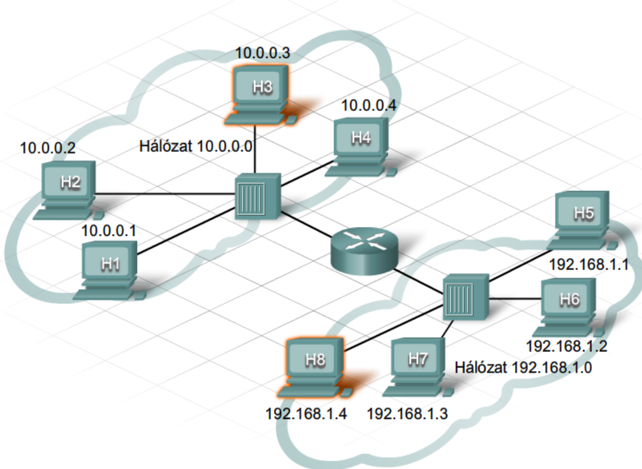
- A helyi hálózaton való kommunikációhoz az szükséges, hogy a számítógépek közös protokollt használjanak.
- A leggyakrabban használt protokoll a vezetékes helyi hálózatokon az Ethernet ipari szabvány.
- Az Ethernet hálózaton minden helyi állomást a fizikai MAC címe azonosítja, ami előre be van állítva az állomás hálózati kártyáján.

Gyakran nagyobb hálózatokat kisebbekre, jobban menedzselhető részekre osztunk réteges hierarchikus tervezést használva, ami a következő rétegekből áll:

- Hozzáférési
- Elosztási
- Központi

Minden rétegnek van egy elsődleges funkciója és hozzárendelt eszközei.

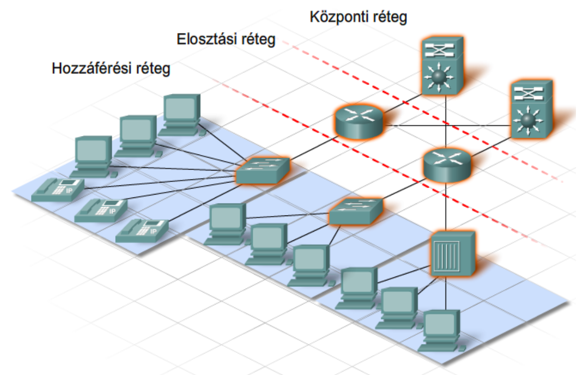




- A hierarchikus modellben az állomások azonosítására logikai IP-címeket használunk.
- Ahhoz, hogy egy független állomásnak csomagot küldjenek, szükséges annak fizikai MAC-címe és a logikai IP-címe.
- A helyi továbbítás esetén, az IP-címek MAC-címre történő feloldásához az ARP protokollt használják.

Hozzáférési réteg:

- Az állomások a hozzáférési rétegben lépnek be a hálózatba.
- Az állomások általában közvetlen Ethernet kábelek használatával csatlakoznak egy hozzáférési réteg eszközhöz, mint például hub vagy kapcsoló.
- A hozzáférési rétegben mind a MAC-címet mind az IP-címet használjuk.



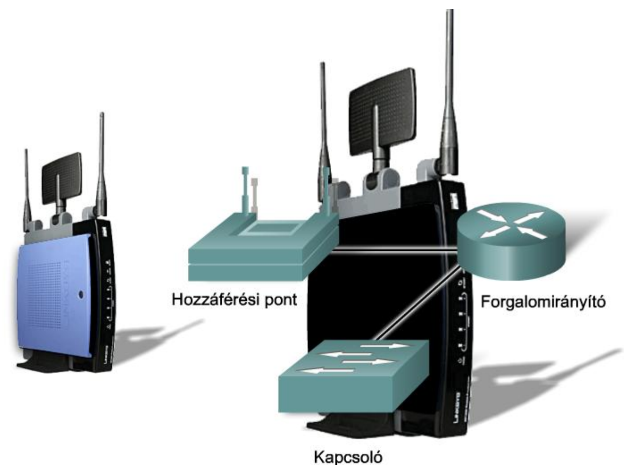
Elosztási réteg:

- Az elosztási réteg független helyi hálózatokat kapcsol össze és közöttük irányítja a forgalmat.
- Egyéni állomások általában nem csatlakoznak közvetlenül elosztás rétegbeli eszközökhöz.
- Az elosztási rétegben a fő hálózati eszközök a forgalomirányítók, melyek a hálózatok közötti csomagküldéshez az IP-címeket használják.

A hálózattervezés első lépése az információgyűjtés a hálózat tervezett használatáról. Ez az információ tartalmazza:

- A hálózathoz csatlakoztatandó állomások száma és típusa
- A használandó alkalmazások
- Megosztási és Internet kapcsolat követelményei
- Biztonsági és titoktartási megfontolások
- Megbízhatósági és rendelkezésre állási elvárások
- Vezetékes és vezeték nélküli kapcsolódási követelmények

- A Cisco ISR-ek és más multifunkciós hálózati eszközök otthoni és kisvállalati hálózatokat kapcsolnak össze azon célból, hogy több állomás erőforrást oszthasson meg és csatlakozhasson az Internethez.
- Egy otthoni hálózati eszköz egy egyszerűsített, olcsó berendezés, amit általában kis hálózatoknál használnak.
- Ezek az eszközök tipikusan egy eszközben biztosítják a kapcsoló, forgalomirányító és vezeték nélküli hozzáférési pont funkciókat.



4. Csatlakozás az internethez

4.1 Az internet fogalma és hogy miként tudunk kapcsolódni hozzá

4.1.1 Mi az internet?

Minden nap emberek milliói cserélnek információt egymással az Interneten keresztül - de mi is pontosan az Internet? Az Internet számítógépes hálózatok világméretű összessége, melyek az információk cseréjéhez egységes szabványokat használva, együttműködnek egymással. Az Internetes felhasználók számára számos mód létezik az információ cseréjéhez: telefonos vezetékeken, optikai kábeleken keresztül, vezeték nélküli átvitellel vagy műholdas kapcsolat segítségével.

További információ

Internetes Szervezetek

Az Internet Society (ISOC) társaság vezető szerepet játszik az Internet jövőbeni kérdéseinek meghatározásában, valamint az Internet infrastruktúrális szabványaiért felelős csoportoknak ad otthont, mint például az Internet Engineering Task Force (IETF) és az Internet Architecture Board (IAB).

Néhány fontosabb szervezet, amely segít az Internet fejlesztésében és irányításában:

ISOC: Internet Society: http://www.isoc.org/isoc/
IAB: Internet Architecture Board: http://www.iab.org/
IETF: Internet Engineering Task Force: http://www.ietf.org/
IRTF: Internet Research Task Force: http://www.irtf.org/
IANA: Internet Assigned Numbers Authority: http://www.iana.org/

Tipp: Az Infoplease jó információforrás az Internet használatának statisztikáiról és erőforrásairól: http://www.infoplease.com/ipa/A0873826.html/

Az Internet, a hálózatok hálózata, amely kapcsolatot teremt a világ minden országának felhasználói között. Jelenleg körülbelül egymilliárd Internet felhasználót tartanak számon világszerte.

Az eddigi hálózatok, melyekről beszéltünk, egy személy vagy szervezet irányítása alatt állnak. Az internet hálózatok összessége, és nem tartozik egy személyhez vagy szervezethez sem. Azonban léteznek nagy nemzetközi szervezetek, melyek közreműködnek az Internet irányításában, így mindenki azonos feltételek mellett használhatja azt.

4.1.2 Az internetszolgáltatók

Bármely otthoni, üzleti vagy szervezeti környezet, amely csatlakozni szeretne az Internethez, valamilyen internetszolgáltató ISP segítségével teheti meg ezt. Az ISP egy vállalat, mely kapcsolatot és támogatást biztosít az Internet eléréséhez. Nyújthatnak egyéb szolgáltatásokat is, úgymint az elektronikus levelezés és webes tárhelyszolgáltatás.

Az ISP-k nélkülözhetetlenek az Internethez való csatlakozáshoz. Senki nem mehet fel az Internetre egy hálózati számítógép használata, illetve egy ISP közreműködése nélkül.

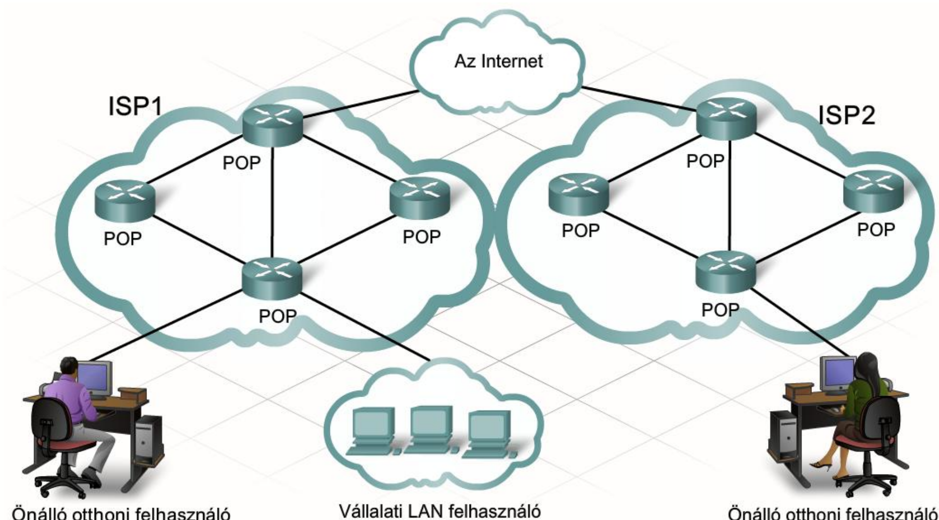
Az internetszolgáltatók méreteikben az egészen kicsitől a nagyon nagyig terjedhetnek, és különbözhetnek a szolgáltatási területek számára nyújtott feltételekben is egymástól. Az ISP-k kisebb földrajzi területeknek is biztosíthatnak korlátozott szolgáltatásokat vagy nyújthatják szolgáltatások széles választékát, melyekkel elláthatnak több millió felhasználóval rendelkező országokat is. Az ISP-k az általuk ajánlott csatlakozási technológiákban és sebességekben is különböznek. A jól ismert ISP-k közé tartoznak például: AOL, EarthLink és Roadrunner.

4.1.3 Az ISP-k kapcsolata az internettel

Az önálló számítógépek és helyi hálózatok a szolgáltatás-elérési ponton (Point of Presence) (POP) kapcsolódnak az internetszolgáltatóhoz. A POP a kapcsolódási pont az ISP hálózata, és a POP által kiszolgált, speciális földrajzi terület között.

Egy ISP-nek több elérési pontja is lehet, a méretének és a kiszolgált terület függvényében. Az ISP-n belül nagysebességű forgalomirányítók és kapcsolók hálózata továbbítja az adatokat a különböző POP-ok között. Többszörös kapcsolat köti össze a különböző elérési pontokat azért, hogy egy kapcsolat meghibásodása vagy túlterheltsége és torlódás esetén másik alternatívát biztosítsanak az adatok áramlásának.

Az ISP-k összeköttetésben vannak más internetszolgáltatókkal annak érdekében, hogy információt tudjanak küldeni a saját hálózatuk határain kívülre. Az Internet nagyon nagy sebességű összeköttetésekből áll, melyek összekapcsolják az ISP-k szolgáltatás-elérési pontjait, illetve a különböző internet-szolgáltatókat egymással. Ezek az összekapcsolódások részei annak a nagyon nagyméretű, és nagykapacitású hálózatnak, amit az Internet Gerinchálózatának nevezünk.



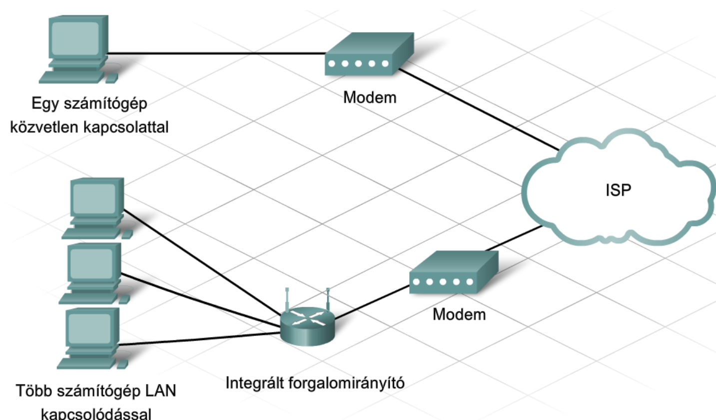
Az elérési ponton csatlakozva az ISP-hez, lehetővé teszi számunkra az általuk nyújtott szolgáltatások igénybevételét és az Internet használatát.

4.1.4 Az internetszolgáltatóhoz való kapcsolódási formák

Az internet-szolgáltatók (ISP) a földrajzi hely és a kívánt sebesség függvényében számos kapcsolódási lehetőséget biztosítanak az Internethez.

A vidéki területekkel szemben, egy jelentősebb városban általában több lehetőségünk van szolgáltatót és kapcsolódási módot választani. Például, a kábeles internet-hozzáférés csak bizonyos nagyvárosi körzetekben lehetséges, ahol a kábeltelevíziós szolgáltatás elérhető. A távoleső helyeken csak betárcsázós vagy műholdas hozzáférésre van lehetőség.

Minden internet-hozzáférési technológia egy bizonyos hálózati eszközt használ, például modemet, az internet-szolgáltatóhoz való csatlakozáshoz. Elképzelhető, hogy ez az eszköz be van építve a számítógépünkbe vagy az ISP külön biztosítja számunkra.



A leggyakoribb esetben egy modemet használunk, amely közvetlen kapcsolatot biztosít egy számítógép és az ISP között.



Azonban, ha több számítógép csatlakozik egyetlen internet-kapcsolathoz, akkor további hálózati eszközökre lesz szükségünk. Ezek közé tartoznak a kapcsolók (switch), melyek több állomást (host) kötnek egy helyi hálózatba és a forgalomirányítók (router), melyek a helyi hálózatunkból az internet-szolgáltatóhoz irányítják a hálózati csomagokat. Egy otthoni hálózati eszköz, például egy integrált forgalomirányító, önmagában képes lehet ezen funkciók ellátására, és vezeték nélküli csatlakozásra is.

A választott internet-elérési technológia számos dologtól függ: kiépítettség, költség, használandó eszköz, átviteli közeg, valamint a kapcsolat sebessége.

A legtöbb bemutatott technológiát mind otthoni, mind kisvállalati környezetben használják. Bérelt vonalakat, tipikusan, üzleti környezetekben, vagy nagyobb szervezetek esetén használnak, de segítségükkel kábel vagy DSL eléréssel nem rendelkező területeknek nyújthatunk nagysebességű hozzáférést.

Betárcsázós

- A leglassabb és legtöbb helyen elérhető szolgáltatás
- Hagyományos, hang-alapú vonalakat használ

Mobiltelefonos modem

- A mobilszolgáltatók által biztosított szolgáltatás
- Aránylag lassú elérésű sebességű, de egyre elterjedtebb

Digitális előfizetési vonal (DSL)

- A legtöbb teflontársaságnál elérhető szolgáltatás
- Nagysebességű digitális vonalat biztosít, telefonvonalakat használva

Kábelmodem

- A legtöbb kábeltelevíziós szolgáltatónál megtalálható
- Nagysebességű kapcsolatot biztosít, kábeltelevíziós hálózatok segítségével

Bérelt vonalak

- A legtöbb telefontársaság által igénybe vehető szolgáltatás
- Nagysebességű kapcsolatot biztosít, dedikált digitális vonalak segítségével
- A bérelt volna leggyakoribb példája a T1
- Elsődlegesen üzleti felhasználásra

Műholdas

- Internetes műholdvevő antennával fogható szolgáltatás
- Közepes nagyságú sebesség érhető el vele, műholdas kapcsolaton keresztül
- Némely vidéki területen a műholdas kapcsolat lehet az egyetlen, betárcsázósnál gyorsabb lehetőség

4.1.5 Az internetszolgálók szolgáltatási szintjei

Internetszolgáltatótól és kapcsolódási típustól függően számos szolgáltatás igénybevételére van lehetőség, például, víruskeresés videó- és tárhelyszolgáltatás. Az ISP-vel kötött szerződés meghatározza az igénybe vehető szolgáltatások típusát és szintjét. A legtöbb internetszolgáltató két különböző szerződési szintet nyújt: otthoni szolgáltatás és üzleti célú szolgáltatás.

Az otthoni szolgáltatások általában nem olyan drágák, mint az üzleti szolgáltatások, és alapvetően korlátozottabb szolgáltatásokat nyújtanak, mint a lassabb kapcsolódási sebesség, csökkentett web tárhely és kevesebb e-mail postafiók. Egy tipikus otthoni szolgáltatás legalább 5 darab E-mail címet foglal magában és további címeket többletköltség esetén vehetünk igénybe.

Az üzleti célú szolgáltatások jóval drágábbak, de gyorsabb kapcsolódási sebességet biztosítanak, továbbá nagyobb webtárhelyet és több használható e-mail postafiókot. Egy ilyen szolgáltatás esetén akár 20, 50 vagy ennél is több e-mail cím használható. Az üzleti szolgáltatások esetén a szolgáltató és az ügyfelek között lehetőség van olyan szerződés kötésére, melyben meghatározzák a hálózat rendelkezésre állásának és a szolgáltatás válaszidejének feltételeit. Ezt a Szolgáltatás Szintje szerződésnek nevezzük (SLA).

Email postafiókok

- Az Internetszolgáltatók általában több felhasználó számára biztosítanak levelezési lehetőséget, egyazon fiókot használva. Ezeket a levelezési címeket szét lehet osztani több felhasználó között, vagy külön üzleti és személyes levelezési célokra is lehet használni.
- A webmail lehetővé teszi a felhasználó számára azt, hogy bármelyik Internetre csatlakozó számítógépről egy böngésző használatával hozzáférjen a leveleihez . Nem szükséges külön erre a célra írt e-mail ügyfélprogram használata.

Személyes weblapok

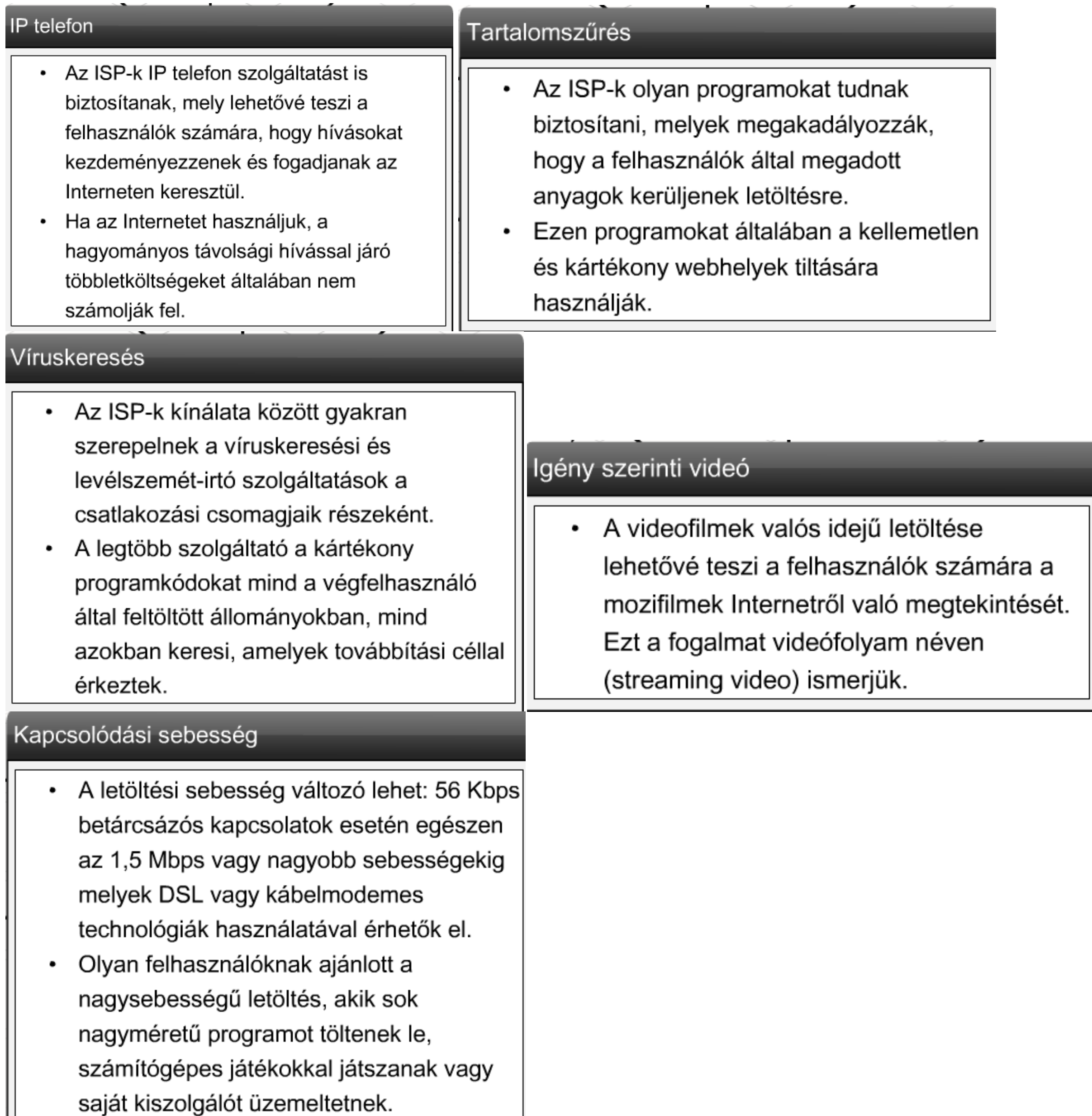
- Személyes webtárhelyet gyakran szolgáltatással együtt biztosítanak. Rendszerint mind a webtárhely mérete mind a forgalmazható adatmennyiség korlátozva van.
- A webhely megtervezése és karbantartása az egyéni tulajdonos feladata.

Webes tárhelyszolgáltatás

- A webkiszolgálóval nem rendelkező szervezetek az internet-szolgáltatók kiszolgálóit használhatják a saját webhelyeik üzemelhetésére. Ez gyakran együttjár a tervezési és karbantartási szolgáltatásokkal.
- A webtárhely szolgáltatások díját rendszerint a webhely mérete és a becsült havi forgalom alapján számítják ki.

Adattárolás

- A különböző vállalkozásoknak lehetősége van a szolgáltatók Internetes tárhely és állománykezelési rendszereinek igénybe vételére, hogy a fontos állományok a hét mind a 7 napján, napi 24 órán keresztül rendelkezésre álljanak.
- Az adattárolási szolgáltatás mértéke a néhány megabájttól a több terrabájt méretig terjedhet.
- Az Internetes adattárolás általában jelszóval védhető.



A hálózati adatátvitel során, az adatot vagy feltöltjük, vagy letöltjük. A letöltés azt jelenti, hogy információ érkezik az Internetről a számítógépünkre, miközben a feltöltés ellentétes irányú folyamatot jelent: az információ számítógépünk felől az Internet felé halad. Amikor a letöltés sebessége különbözik a feltöltés sebességétől, azt aszimmetrikus kapcsolatnak nevezzük. Amikor az átvitel mértéke megegyezik mindkét irányban, szimmetrikus kapcsolatról beszélünk. Az ISP-k aszimmetrikus és szimmetrikus szolgáltatásokat is nyújthatnak.

Aszimmetrikus:

- Leggyakrabban otthoni kapcsolatok esetén használják.
- A letöltési sebességek gyorsabbak, mint a feltöltés sebességek.
- Olyan felhasználóknak szükséges, akik jelentősen többet töltenek lefelé, mint felfelé.
- A legtöbb Internet felhasználónak, különösen azoknak, akik grafikai vagy multimédiás adatokat használnak az Interneten, nagy letöltési sávszélességre van szükségük.

Szimmetrikus:

- Leggyakrabban üzleti felhasználásra vagy az Interneten egyénileg üzemeltetett kiszolgálók esetén használják.
- Akkor használják, amikor nagy mennyiségű grafikai, multimédiás vagy videó anyagokat kell feltölteni.
- Mindkét irányban, egyenlő mértékben képes továbbítani nagy mennyiségű adatot.

4.2 Információ küldése az interneten keresztül

4.2.1 Az internet protokoll (IP) jelentősége

Az állomásoknak, az interneten való kommunikációjukhoz, Internet Protokollt (IP) használó szoftvert kell futtatniuk. Az IP protokoll tagja egy olyan protokoll készletnek, amelyet egységesen TCP/IP-nek (Transmission Control Protocol / Internet Protocol) hívunk. Az Internet Protokoll (IP) csomagokat használ az adatok szállításához. Akár egy Internetes videójátékot játszunk, csevegünk egy barátunkkal, levelet küldünk vagy keresünk a weben, az információ, melyet küldünk és fogadunk, IP csomagok formájában kerül átvitelre.

Minden IP csomagnak érvényes forrás és cél IP címmel kell rendelkeznie. Érvényes cím információ nélkül a küldött csomagok nem érik el a célállomást. Illetve, a visszatérő csomagok nem találnak vissza a kiindulási helyükre.

Az IP meghatározza a forrás és cél IP címek szerkezetét. Megadja, hogyan kell kell használni ezeket a címeket a csomagok irányításához, egyik állomásból vagy hálózatból a másikba.

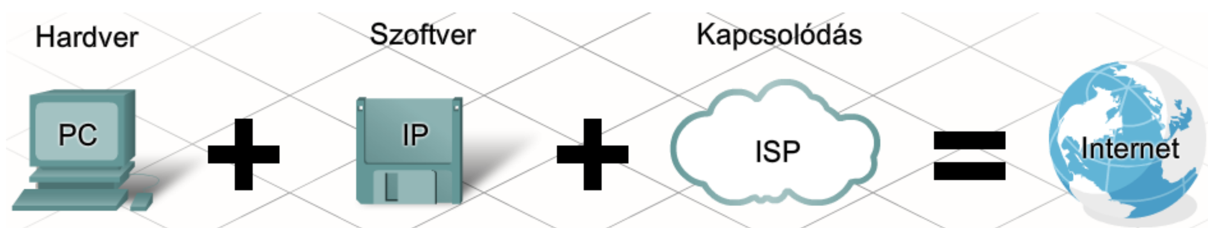
Request For Comments

Az RFC-k számozott dokumentumok, melyek protokollokat és más az internet működését meghatározó szabványokat definiálnak. Minél magasabb értékű az RFC azonosítószáma, annál újabb. Az RFC dokumentumokat az IETF szervezethez nyújtják be, ahol egy felülvizsgálati folyamaton mennek át. A felülvizsgálat alatt, a következő minősítő szinteket járják be:

- Javaslat (belépő szinten)
- Tervezet (kezdeti tesztelés)
- Szabvány (teljesen elfogadott)

IETF RFC webhely:
http://www.ietf.org/rfc.html

Minden, az interneten használt protokollt, beleértve az IP-t, számozott szabvány dokumentumokban határoztak meg, melyeket RFC (Request for Comments) dokumentumoknak hívnak.



Egy IP csomag elején a fejrész van, ami a forrás- és célcímeket tartalmazza. Valamint vezérlő információkat is tartalmaz, melyek leírják az útvonalába kerülő hálózati eszközök (például forgalomirányítók) számára a csomag rendeltetését, és segítik annak irányítását a hálózaton. Az IP csomagot néha datagramnak is nevezik.

Az IP címnek egyedinek kell lennie az Interneten. Léteznek olyan szervezetek, melyek az IP címek kiosztásának irányításáért felelősek, így nincs ismétlődés a címek között. Az Internetszolgáltatók IP

címek tartományait, blokkjait kapják egy helyi, nemzeti vagy regionális Internetes hivataltól. A szolgáltató felelőssége a kapott címek kezelése és az egyes végfelhasználókhoz rendelése.

Az otthoni számítógépek, kisvállalatok és más szervezetek az Internetszolgáltatójuktól kapják az IP címüket. Általában ezt a beállítást automatikusan kapják, amikor a felhasználók csatlakoznak az ISP-hez Internet elérés végett.

4.2.2 Hogyan kezelik az adatokat az internetszolgáltatók

Mielőtt küldésre kerülnének az Interneten, az üzeneteket csomagokra osztják. Az IP csomag mérete 64 és 1500 bájt között lehet az Ethernet hálózatokban, és nagyrészt felhasználói adatokat tartalmaznak. Egy egyszerű 1 MB méretű zeneszám letöltéséhez több mint 600 darab 1500 bájtos csomagra van szükségünk. Minden egyes csomagnak rendelkeznie kell egy forrás- és egy célcímmel.

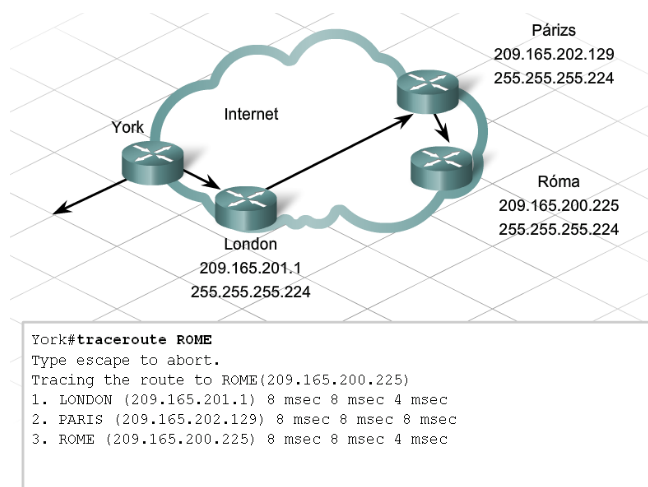
Amikor egy csomagküldésre kerül az Interneten, az ISP meghatározza, vajon a csomagot egy, az ISP hálózatában lévő, helyi szolgáltatáshoz címezték, vagy egy másik hálózat távoli szolgáltatásához.

Minden ISP rendelkezik egy vezérlő létesítménnyel, melyet Hálózatüzemeltető Központnak (NOC) neveznek. Az NOC általában a hálózati forgalom vezérléséért felelős, és helyet ad olyan szolgáltatásoknak, mint az E-mail vagy web üzemeltetés. Az NOC vagy valamelyik szolgáltatás-elérési pontnál található, vagy egy teljesen különálló létesítményben foglal helyet az ISP hálózatán belül. Az olyan csomagok, melyek helyi szolgáltatásokat akarnak igénybe venni, általában a NOC-hez továbbítódnak és soha nem hagyják el az ISP hálózatát.

Az ISP-k minden egyes szolgáltatás-elérési pontján megtalálható forgalomirányítók a csomagok célcímeit használják az Interneten való áthaladás legjobb útvonalának kiválasztásához. Az ISP POP felé küldött csomagjainkat forgalomirányítók továbbítják az ISP-nk hálózatán keresztül, azután más ISP-k hálózatain is. Egyik forgalomirányítótól a másikhoz kerülnek, míg végül elérik a végső céljukat.

4.2.3 Csomagok továbbítása az Interneten keresztül

Léteznek hálózati segédprogramok, melyekkel tesztelni lehet a cél-eszközzel való kapcsolódást. A *ping* segédprogramot végpontól végpontig terjedő kapcsolat tesztelésére használhatjuk a forrás- és cél állomás között. Megméri a tesztcsomag oda-vissza útja közben eltelt időt, és megállapítja az átvitel sikerességét. Azonban, ha a csomag nem éri el a célállomást, vagy túl nagy késleltetést szenved az útja során, nincs mód arra, hogy kiderüljön a probléma helye.



Hogyan lehetséges megállapítani, mely forgalomirányítókat hagyta el a csomag és melyek az útvonal problémás helyei?

A *traceroute* segédprogram lenyomozza, végigköveti a forrástól a célhelyig bejárt útvonalat. Minden egyes forgalomirányító, melyen a csomag áthalad, egy-egy ugrásnak felel meg. A *Traceroute* megjeleníti az egyes ugrásokat az út során, és az ugrásokhoz szükséges időt is. Ha probléma következik be, a megjelenített idő és a csomag által addig bejárt út segít megállapítani, hol veszett el,



vagy szenvedett késleltetést csomagunk. A *traceroute* segédprogramot *tracert*-nek nevezzük a Windows-os környezetben.

Ezenkívül létezik néhány vizuális *traceroute* program, amelyek képesek grafikusan megjeleníteni a csomag által bejárt utat.

4.3 Hálózati eszközök egy NOC-ban

4.3.1 Internetes felhő

Amikor a csomagok az Interneten keresztül utaznak, számos hálózati eszközön haladnak keresztül.

Az Internetet forgalomirányítók hálózatának is elképzelhetjük, melyek egymással összeköttetésben állnak. Nagyon gyakran alternatív útvonalak is léteznek a forgalomirányítók között, ezért elképzelhető, hogy a csomagok különböző útvonalakat használnak ugyanazon forrás és a cél között.

Ha probléma lép fel a forgalomban a hálózat bármely pontján, a csomagok az alternatív útvonalakat automatikusan igénybe veszik.

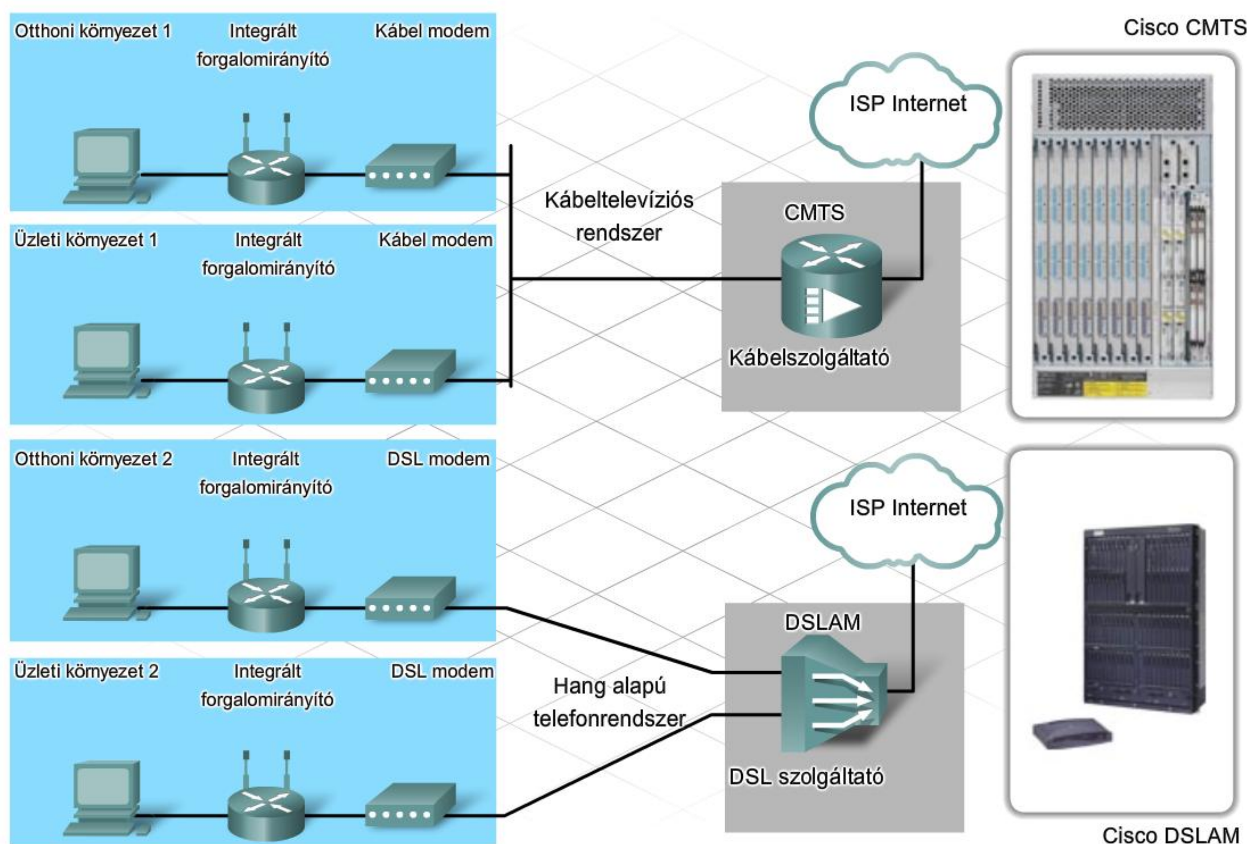
Egy diagram, amelyen minden hálózati eszköz és a köztük lévő összeköttetések szerepelnének, nagyon összetett lenne. Ráadásul, a forrás és cél közötti végleges útvonal általában nem fontos, csak az, hogy a forrás képes legyen kommunikálni a célállomással. Emiatt, egy hálózati diagramon egy felhő gyakran jelenti az Internetet vagy más összetett hálózatot, a bennük lévő kapcsolatok részleteit elfedve. A felhő lehetővé teszi az egyszerű ábrák esetén, hogy az csak a forrás és a cél állomásokra összpontosítson, még akkor is, ha számos eszköz szerepelne az útvonalon.

4.3.2 Eszközök az internetfelhőben

Sem az Internet felhő esetében, sem az ISP-knél található eszközök között, nem a forgalomirányítók az egyedüli eszközök. Az Internetszolgáltatóknak fogadni és kézbesíteni kell a végfelhasználók információit, valamint részt kell venniük az Internet működésében.

Azon eszközöknél használt technológiának, melyek kapcsolódást biztosítanak a végfelhasználóknak, meg kell egyeznie a végfelhasználó által használt eszköz technológiájával, a sikeres csatlakozás érdekében. Például, ha a végfelhasználó DSL technológiát használ a kapcsolódáshoz, akkor az ISP-nek rendelkeznie kell egy DSL Access Multiplexerrel DSLAM, ezen kapcsolat fogadásához. A kábel modemes csatlakozáshoz, az ISP-nek rendelkeznie kell egy Cable Modem Termination Rendszerrel CMTS. Némely ISP még fogad modemen keresztül indított analóg hívásokat és ezen felhasználók támogatásához rendelkeznek modemek blokkjaival. Azon internetszolgáltatóknak, melyek vezeték nélküli szolgáltatásokat nyújtanak, vannak vezeték nélküli híd berendezéseik.

Az internet-szolgáltatónak képeseknek kell lenniük más szolgáltatókkal való csatlakozásra és adattovábbításra is. Számos különböző technológiát használnak ezen célok eléréséhez, mindegyik különleges berendezést és konfigurációt igényel a működéséhez.



Egy ISP-nél használt készülékek típusa attól függ, milyen technológiájú hálózatban vesznek részt. A forgalomirányítók és kapcsolók teszik ki ezen eszközök nagy részét. De ezen eszközök sokban különböznek az otthoni vagy kisvállalati környezetekben találhatóaktól.

Az ISP-k által használt hálózati eszközök képesek nagyon gyorsan kezelni óriási mennyiségű hálózati fogalmat is. Közel 100%-os üzemidőben kell működniük, mivel egy kulcsfontosságú ISP berendezés meghibásodása katasztrofális következményekkel járhat a hálózati forgalomban. Ezen okból, a legtöbb ISP által használt eszköz csúcstechnológiás, nagysebességű és redundáns (tartalék) működésű.

Ezzel szemben, az otthoni vagy kisvállalati környezetben használt eszközök kevésbé fejlettek, alacsonyabb sebességűek és nem képesek kezelni nagyméretű hálózati forgalmat. Az integrált forgalomirányítók a következő funkciókra lehetnek képesek: Vezeték nélküli LAN hozzáférési pont, forgalomirányítás, tűzfal és többféle címzési lehetőség. Egy integrált forgalomirányító képes ezen feladatok közül némely, vagy az összes ellátására.

4.3.3 Fizikai és környezeti követelmények

Az internet-szolgáltatóknál és az otthoni vagy kisválalkozásoknál található hálózatok felépítése nagyon különböző.

Egy otthoni vagy kisvállalati hálózat viszonylag kevés felhasználónak biztosít kevés szolgáltatást. Az Internet-csatlakozást egy szolgáltatótól vásárolják. A hálózati forgalom kis mennyiségű, és nem biztosítottak szállítási szolgáltatások.

Az Internetszolgáltatók a felhasználók széles körének biztosítanak szállítási és egyéb szolgáltatásokat. Több különböző eszközre van szükség a felhasználókkal való kommunikáció biztosítása érdekében. Ahhoz, hogy részt vegyenek egy szállítási hálózatban, tudniuk kell kapcsolódni más Internetszolgáltatókhoz. Nagyméretű hálózati forgalmat bonyolítanak, a terhelés kezeléséhez nagyon megbízható eszközökre van szükségük.

Annak ellenére, hogy ezen hálózatok nagyon különbözőnek tűnnek, mindkettőnek szüksége van olyan környezetre, ahol a berendezések megbízhatóan és megszakítás nélkül üzemelhetnek. A követelmények ugyanazok, de a működés mértéke eltér: az otthonokban egyetlen fali konnektor képes ellátni az eszközöket, ellenben egy szolgáltatónál az energia szükségleteket előre meg kell tervezni és megfelelően kivitelezni.

Az egyik fő különbség a szolgáltatók és az otthoni hálózatok között, a kiszolgálók jelenléte. A legtöbb otthoni felhasználó nem üzemeltet kiszolgálót, még a kisvállalatok esetében is csak elenyésző számú fordul elő. Az ISP-k szolgáltatásaira támaszkodnak, mint például e-mail, webcím-hozzárendelés és webtárhely. Egy Internetszolgáltatónak nem csak a hálózati eszközök fizikai követelményeit kell figyelembe vennie, hanem a kiszolgálókét is, melyeket üzemeltetnek.

Az egyik legfontosabb tényező az elektromos eszközök esetében a megbízható és állandó áramellátás biztosítása. Sajnos, a rendelkezésre álló áramellátás nem mindig megbízható, ami a hálózati eszközök problémájához vezethet. Az ISP-k áramellátás szabályozó berendezéseket telepítenek, melyek tartalék biztonsági akkumulátorokat tartalmaznak, így fenntartják a folyamatos tápellátást a fő áramhálózat meghibásodása esetén is. Az otthoni és kisvállalatok esetében, az olcsó szünetmentes tápegységek (UPS) és biztonsági akkumulátorok általában elegendőek a hozzájuk csatlakoztatott viszonylag kevés eszköz ellátására.

A környezeti tényezőket, úgymint a hőmérséklet és a páratartalom, ugyancsak figyelembe kell vennünk egy hálózat tervezésekor. Éppen azért, az ISP-k által használt nagyszámú eszköz és a felhasznált energia miatt, a legfejlettebb légkondicionáló berendezésekre van szükség a hőmérséklet szabályozásához. Az otthonokban és kisvállalati környezetekben általában elegendő a szokványos légkondicionálás, fűtés és páratartalom-szabályozás.

A kábelmenedzsment egy másik olyan terület, melyet mind az otthonok/kisvállalatok, mind az internet-szolgáltatók esetében figyelembe kell venni. A kábeleknek védelmet kell nyújtani a fizikai sérülések ellen, és oly módon kell őket rendezni, hogy az segítse az esetleges hibaelhárítási folyamatokat. A kisebb hálózatoknál csekély számú kábel van jelen, ám az ISP hálózatokban több ezer kábel kezelésével kell számolni. Ezen kábelek közé a rézkábeleken kívül, még az optikai szálas és a tápellátásért felelős kábelek is beletartoznak.

Mindezen tényezőkre, úgymint az áramellátás, környezet és kábelmenedzsment tekintettel kell lenni bármilyen méretű hálózat építésekor. Egy ISP és egy otthoni hálózatban nagy különbségek vannak a méretekben, emiatt a követelményekben is. A legtöbb hálózat ezen két szélsőség közé sorolható.

4.4 Kábelek és csatlakozók

4.4.1 Gyakori hálózati kábelek

Annak érdekében, hogy a kommunikáció létrejöjjön, egy forrásnak, egy célnak és valamilyen csatornának kell lennie. Egy csatorna vagy átviteli közeg útvonalat biztosít, melyen információ küldhető. A hálózatok világában az átviteli közeg általában valamilyen fizikai kábel. A vezeték nélküli hálózatok esetében az elektromágneses sugárzás az átviteli közeg. A forrás és cél közötti kapcsolat lehet direkt (közvetlen) és indirekt, illetve, többféle típusú átviteli közeget is érinthet.

Többféle különböző típusú hálózati kábel létezik a hálózati központok (NOC) vagy helyi hálózatok eszközeinek összekötésére.

Két fajta fizikai kábelezés létezik. A fém alapú kábelek, általában rézből készülnek, és a rájuk adott elektromos impulzusok hordozzák az információt. Az optikai szálas kábelek, melyek üvegből vagy műanyagból készülnek, fény impulzusokat használnak az információ átviteléhez.

Csavart érpár

A korszerű Ethernet technológiában általában egy bizonyos típusú réz kábelt használnak az eszközök összeköttetéséhez, melyet csavart érpárként (TP) ismerünk. Mivel az Ethernet a legtöbb helyi hálózat alapvető szabványa, a csavart érpár a legtöbbször előforduló hálózati kábeltípus.

Koaxiális kábel

A koaxiális kábelt általában rézből vagy alumíniumból készítik és a kábeltelevíziós társaságok használják őket a szolgáltatásaik biztosításához. Használják őket a műholdas kommunikációs rendszerek eszközeinek összekötéséhez is.

Optikai kábel

Az optikai szálas kábelek üvegből vagy műanyagból készülnek. Nagyon nagy sávszélességgel bírnak, így hatalmas mennyiségű adat átvitelére képesek. Ezeket gerinchálózatokban, nagyméretű vállalati környezetekben és adattároló központok esetében használják. A telefonos vállalatok is számos területen alkalmazzák.

4.4.2 Csavart érpáras kábelek

A csavart érpáras kábelek egy vagy több szigetelt rézvezetékből állnak, melyeket páronként egymással összecsavartak és egy külső védőburkolattal láttak el. Mint minden réz alapú kábel, a csavart érpáras kábelek is elektromos impulzusokat használnak az adatátvitelhez.

Az adatátvitel érzékeny az úgynevezett interferenciára vagy zajra, amely csökkentheti a kábel által nyújtott adatátvitel mértékét. A csavart érpáras kábelek bizonyos típusú zajokra érzékenyek, például az elektromágneses interferenciára (EMI).

Az egyik interferencia forrás, melyet áthallásként ismerünk, akkor lép fel, amikor különböző kábelek nagy távolságon keresztül vannak egymáshoz kötegelve. Az egyik kábelen haladó jel kiszivárog és belép a szomszédos kábelekbe.

Amikor az adatátvitel interferencia, például áthallás, következtében sérül, újra kell küldeni az adatokat. Ez csökkentheti a közeg adatátviteli kapacitását.



A csavart érpáras kábeleknél, az egységnyi hosszon mérhető csavarások száma befolyásolja a kábel, interferenciával szemben való ellenállását. A kevésbé ellenálló, de a telefonos átvitelnek megfelelő csavart érpáras kábeleket CAT 3 kábeleknek nevezik, és 1 láb hossz alatt 3-4 csavarást végeznek rajtuk. Az adatátvitelnek megfelelő kábel, melyet CAT5-ként ismerünk, 3-4 csavarással rendelkezik egyhüvelyknyi hosszon, így jóval ellenállóbb az interferenciával szemben.

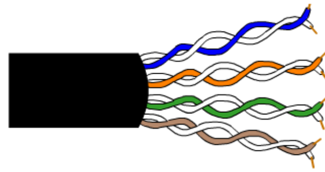
Háromféle típusú csavart érpáras kábelt különböztetünk meg: árnyékolatlan csavart érpáras kábel, érpáronként árnyékolt csavart érpáras kábel, csak közösen árnyékolt csavart érpáras kábel.

Az árnyékolatlan csavart érpár (UTP) a leggyakrabban előforduló hálózati kábeltípus Észak Amerikában és sok más területen egyaránt. Az árnyékolt kábelek (ScTP és F-UTP) szinte kizárólag csak európai országokban használtak.

Az UTP kábel olcsó, nagy sávszélességű és könnyen telepíthető. Ezt a kábelt munkaállomások, számítógépek és hálózati eszközök összekötésére használják. A kábel burkolatában lévő érpárok száma változhat, de a leggyakrabban 4 érpárral találkozunk. Az egyes érpárak különböző színkóddal vannak jelölve.

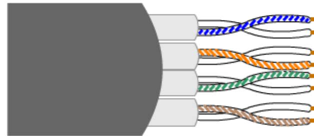
Az évek alatt több különböző kategóriájú UTP kábelt fejlesztettek ki. Minden kategóriát azért fejlesztettek ki, hogy bizonyos technológiát támogasson és legtöbbjükkel már nem találkozunk az otthoni vagy irodai környezetekben. A leggyakrabban előforduló kábelketegóriák, a 3, 5, 5e, és 6. Elektromos környezetek esetén, mint egy zajos gyártelep, ahol az EMI és az RFI erős, árnyékolás szükséges a kommunikáció biztosításához. Ebben az esetben olyan kábelt szükséges használnunk, mint a csak közösen árnyékolt érpár (STP) vagy az egyenként árnyékolt érpár (ScTP). Sajnos, mind az STP, mind az ScTP nagyon drágák és kevésbé rugalmasak, valamint további intézkedéseket igényelnek, mivel az árnyékolás nehezebbé teszi használatukat.

Minden adatszállításra alkalmas kategóriájú UTP kábel hagyományosan egy RJ-45-ös csatlakozóval végződik.



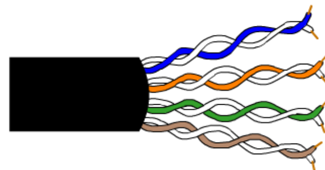
Cat 3-as UTP kábel

- Hang alapú kommunikációra használják.
- Leggyakrabban telefon vonalak esetén használják.



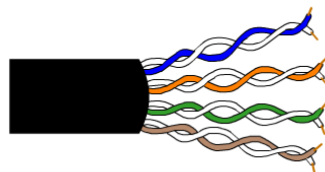
Cat 7 (ScTP) kábel

- Adatátvitelre használják.
- Az egyes érpárokat árnyékoló fóliába csomagolják, majd mind a négy érpárat egy közös árnyékoló réteggel vonják be.
- Támogatja az 1000 Mbps - 10 Gbps sebességeket, azonban ez utóbbi használatára nem ajánlott.



Cat 6 UTP kábel

- Adatátvitelre használják.
- A kábel belsejében az egyes érpárokat szigetelőanyag segítségével különítik el egymástól, emiatt képes nagyobb átviteli sebességre.
- Támogatja a 1000 Mbps - 10 Gbps sebességeket, bár ez utóbbi használatára nem ajánlott.



Cat 5 és 5e kategóriájú UTP kábel

- Adatátvitelre használják.
- A Cat 5 támogatja a 100 Mbps sebességet, valamint képes 1000 Mbps-ra is, azonban ennek használatára nem ajánlott.
- A Cat 5e támogatja az 1000 Mbps átviteli sebességet.

4.4.3 Koaxális kábel

Akár a csavart érpárak esetében, a koaxiális kábel (vagy koax) is elektromos jelek segítségével hordozza az adatokat. Jobb árnyékolást biztosít az UTP-vel szemben, így alacsonyabb a jel-zaj aránya, ami által több adat vihető át rajta. Gyakran használják arra, hogy a televíziót összekössék a jelforrással, legyen az fali kábel-TV aljzat, műholdas TV vagy hagyományos antenna. Szintén használják NOC-kban internet fejállomások (CMTS) és nagysebességű interfészek csatlakoztatására.

Annak ellenére, hogy a koax jobb adatátviteli tulajdonságokkal rendelkezik, a helyi hálózati felhasználás esetében a csavart érpáras kábelezés váltotta fel. A váltás okai között szerepel - az UTP-vel szemben - a koax fizikailag nehezebben telepíthető, jóval drágább és a hibaelhárítása is körülményesebb.

Kábelcsatlakozók:

- A koax kábelt általában BNC vagy F-típusú csatlakozókkal zárjuk le.
- A BNC egy betekerhető csatlakozás, mely erős összeköttetést biztosít.
- Az F-típusú csatlakozókat rá kell csavarni a megfelelő aljzatra.

Fonat

- Egy alumíniumból készült fémfonat vagy fólia, amely védelmet nyújt az EMI ellen.

Szigetelő

- A szigetelő, mely általában műanyagból készül, védelmet nyújt az interferencia ellen, és szilárdságot ad a kábelnek, rugalmassá téve azt.

Vezető

- Egy önálló központi vezető, amelyet általában rézből készítenek, bár alumíniumot is használhatnak hozzá.

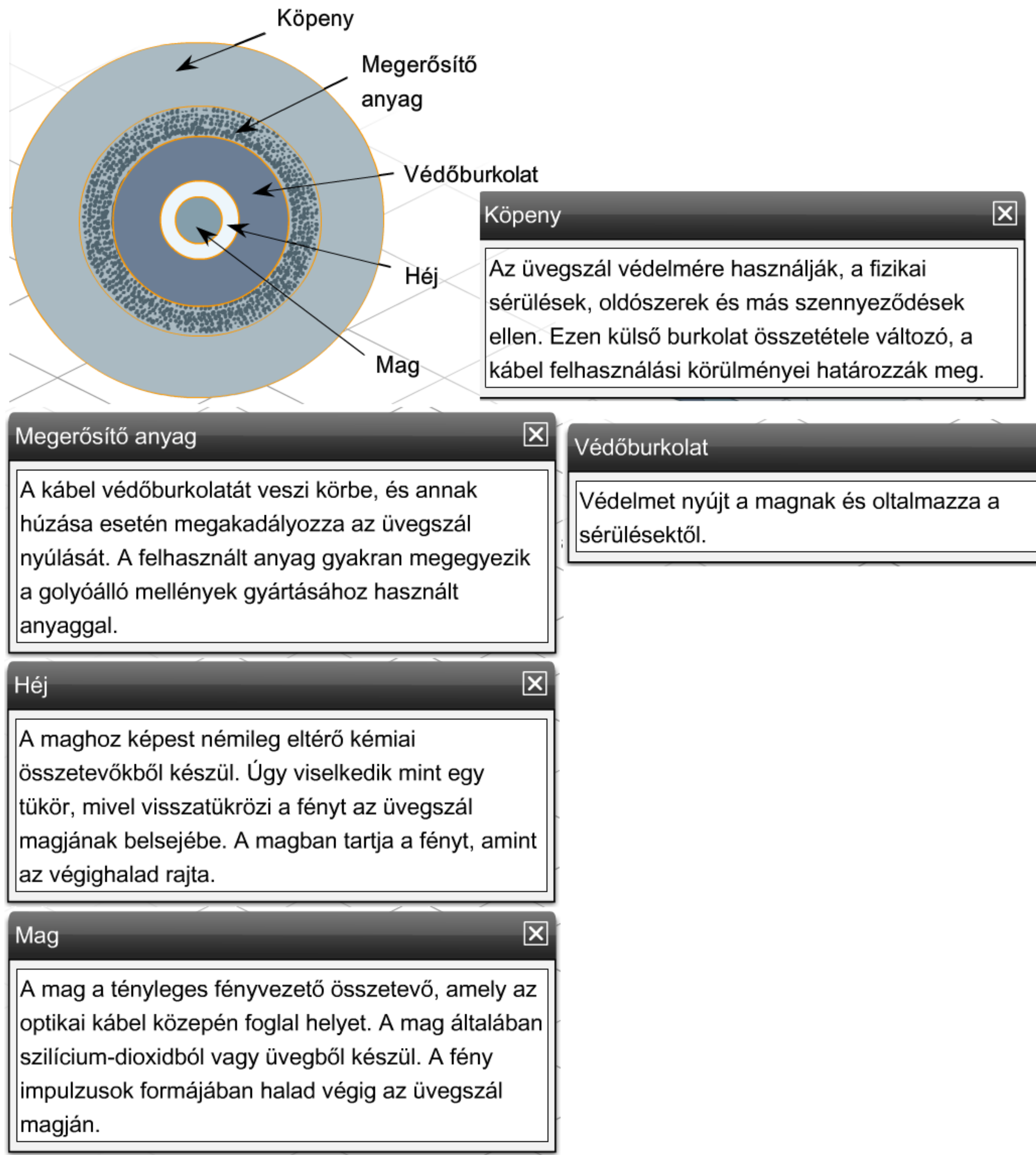
4.4.4 Optikai szálas kábelek

A csavart érpárral és a koaxiális kábellel ellentétben, az optikai kábelek fényimpulzusok segítségével továbbítják az adatokat. Bár normális esetben az otthoni vagy kisvállalkozási környezetekben az optikai kábel nem lelhető fel, a vállalati területeken és nagy adattároló központokban elég széles körben alkalmazzák.

Ezek a kábelek vagy üvegből vagy műanyagból készülnek, és nem vezetik az elektromosságot. Ez azt jelenti, hogy teljesen érzéketlenek az elektromágneses impulzusokra (EMI), és alkalmasak, olyan környezetekben való telepítésre, ahol az interferencia problémát okoz.

Ezenkívül, az optikai kábelek nagy hálózati-sávszélességgel bírnak, amely ideálissá teszi őket a nagysebességű gerinchálózatok kialakítására. Az optikai kábeles gerinchálózatokat a legtöbb vállalatnál, illetve az ISP-k Internetes gerinchálózata esetén találhatunk.

Minden optikai "aramkör" ténylegesen két optikai kábelből áll. Az egyiket az adatok küldésére, a másikat vételére használják.



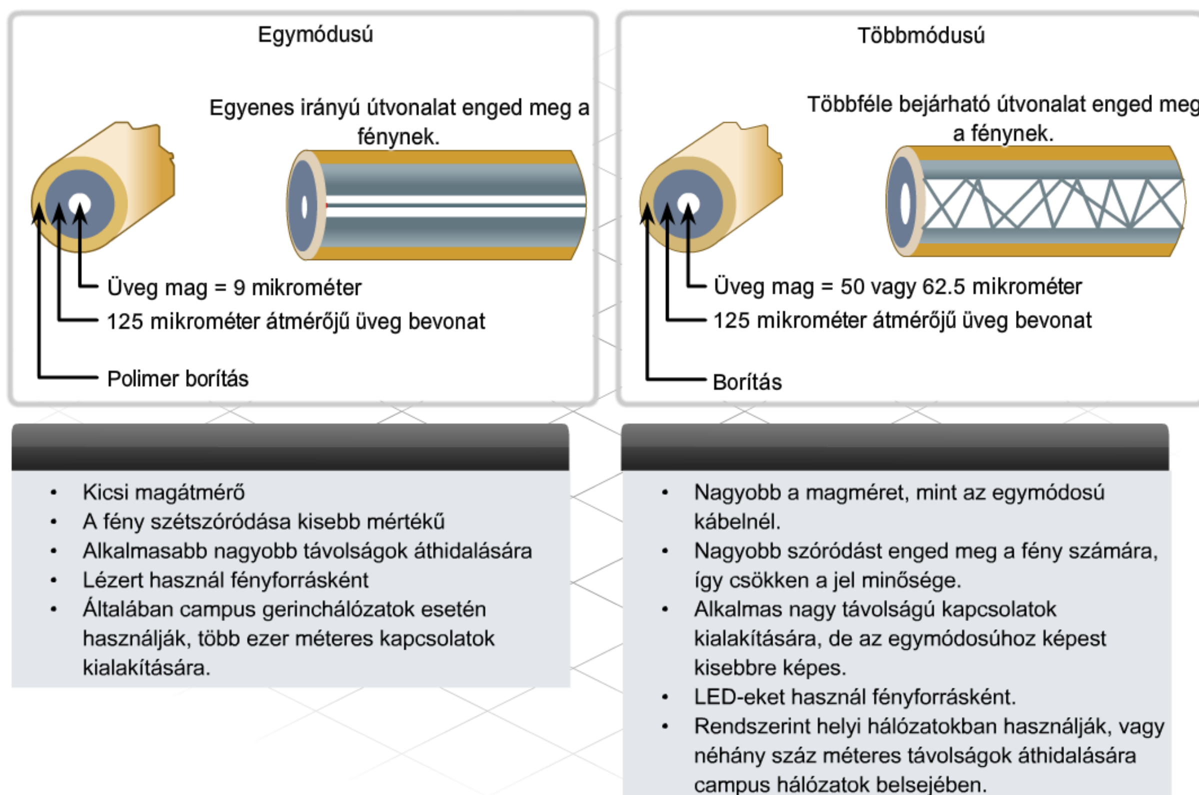
Kétféle típusú optikai kábel van: a többmódusú és az egymódusú.

Többmódusú

A két típus közül, a többmódusú a kevésbé költséges és szélesebb körben használt. A fényforrás, amely a fényimpulzusokat állítja elő, általában egy LED. Azért nevezik többmódusúnak, mert egyidejűleg több fénysugár halad át rajta, adatokat hordozva. Az egyes fénysugarak másféle utat járnak be a többmódusú kábel magjában. A többmódusú kábelek általában 2000 méter távolságig alkalmasak kapcsolatok kialakítására. Azonban, a technológia állandó fejlesztése folyamán, ez a távolság növekszik.

Egymódusú

Az egymódusú kábeleket oly módon tervezik, hogy a fény kizárólag egy utat bejárva haladhat végig az optikai szálon. Az egymódusú kábelek esetén használt fényforrás általában egy LED lézer, amely jóval költségesebb és intenzívebb jelet biztosít, mint a hagyományos LED-ek. A LED lézer erőssége miatt, sokkal nagyobb adatátviteli rátával rendelkezik és nagyobb távolságok áthidalására alkalmas. Az egymódusú kábelek körülbelül 3000 méter távolságig működnek és a gerinchálózati kábelezésben fordulnak elő, például a különböző NOC központok összekötésénél. Itt is meg kell említenünk, hogy a technológia fejlesztése folyamatosan növeli az áthidalható távolságot.



4.5 Csavart érpáras kábelek használata

4.5.1 Kábelezési szabványok

A kábelezés bármely hálózat szerves részét képezi. Kábelek telepítésekor fontos követni a kábelezési szabványokat, melyeket azért fejlesztettek ki, hogy az adathálózatok kölcsönösen megállapított teljesítmény szintek között tudjanak működni.

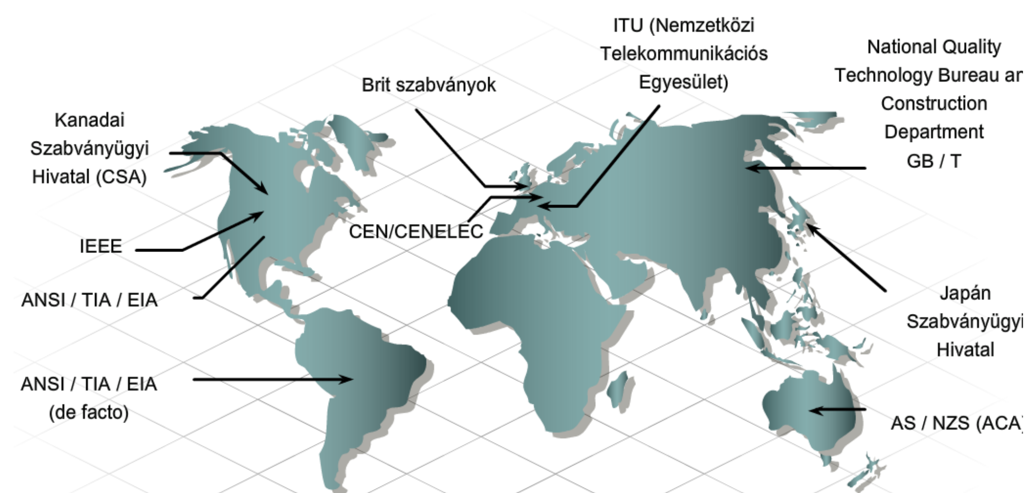
A kábelezési szabványok előírások sorozata, melyeket a telepítésnél és a tesztelésnél kell követni. A szabványok előírják az egyes környezetekben használandó kábeltípusokat, vezető anyagokat, bekötési módokat, a vezetékek méretét,

A világszerte használt Ethernet technológia miatt, előrelátóan fektettek be abba, hogy a struktúrát kábelezést kezdték el használni, az eszközök energia ellátására. 1999-ben, az IEEE elkezdte az Etherneten keresztül szolgáltatott tápfeszültség szabványának kidolgozását. Mára a szabványt IEEE 802.3af-2003 néven ismerjük. Arra használják, hogy 48 volt egyenfeszültséget küldjenek Ethernet adatfolyammal együtt 4 érpáras UTP vagy STP kábelen keresztül. A Power Over Ethernet (POE) - lehetővé teszi a hálózati mérnökök számára a végponti eszközök rugalmas elhelyezhetőségét, gondolunk itt vezeték nélküli hozzáférési pontokra, videó kamerákra, IP telefonokra, mivel így nincs szükség az eszközök közelében elhelyezett fali áramcsatlakozóra.

árnyékolást, kábelhosszt, a csatlakozók típusát és a teljesítmény-korlátokat.

Több különböző szervezetet érint a kábelezési szabványok létrehozása. Míg ezen szervezetek közül néhánynak csak helyi hatásköre van, számos más szervezet szabványát világszerte használják.

Néhány szervezet és az általuk irányított területek listája a képen látható.

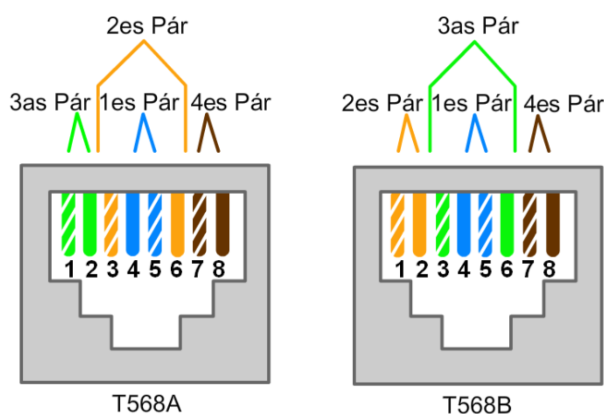


4.5.2 UTP kábelek

A csavart érpár a leggyakrabban használt kábeltípus hálózatok építésekor. A TIA/EIA szervezet két különböző mintát, bekötési sémát határozott meg: T568A és T568B. Mindegyik huzalozási rendszer meghatározza a kábelvégek csatlakozási pontjait, vagy azok sorrendjét.

A két séma hasonló, kivéve, hogy a négy érpárból kettő, fordítva van bekötve. Az ábrán láthatók a kábel színkódjai és az érpárak fordított bekötési sorrendje.

Egy hálózati telepítés során az egyik kábelezési sémát (T568A vagy T568B) érdemes választani, és aszerint dolgozni. Nagyon fontos, hogy munkánk során ugyanazon sémát kövessük minden kábelvégnél. Ha egy meglévő hálózatban kell dolgoznunk, kövessük a már használt kábelezési sémát.



A T568A és T568B sémákat használva, két különböző típusú kábel készíthető: egyeneskötésű illetve keresztkötésű. Mindkét kábeltípus megtalálható az adathálózatokban.

Egyeneskötésű Kábelek

Az egyeneskötésű kábel a leggyakrabban előforduló típus. A kábel mindkét végén azonos kötési sorrendet használ. Más szavakkal, ha egy kábel egyik vége T568A szabványú, akkor a másik vége is T568A. Ha T568B használ az egyik végen, T568B-nek kell lennie a másik végen is. Ez a vezetékek sorrendje szempontjából azt jelenti, hogy minden egyes szín ugyan abban sorrendben van mindkét kábelvégen.

Azt, hogy melyik típusú egyeneskötésű kábelt (T568A vagy T568B) használják a hálózatban, a hálózat által használt kábelezési séma határozza meg.

Keresztkötésű kábel

Egy keresztkötésű kábel mindkét sémát használja. Ugyanazon kábel egyik végén T568A, a másikon T568B a használt séma. Ez azt jelenti, hogy az egyik végen található bekötési sorrend nem egyezik meg a másik vég bekötési sorrendjével.

Mind az egyeneskötésű, mind a keresztkötésű kábelt más-más céllal használják a hálózatokban. Két eszköz összekötéséhez használandó kábel típusa függ attól, hogy az eszközök mely érpárakat használják adásra és vételre.

Az adási és vételi funkciók a csatlakozó meghatározott pontjaihoz vannak rendelve. Az ellenoldalnak megfelelő adási és vételi csatlakozópontokat az eszköz határozza meg.

Két összekötött eszköz, melyek nem ugyanazon érintkezőket használják adásra és vételre, ellentétes jelkiosztással csatlakozó eszközöknek nevezzük. Egyeneskötésű kábelre van szükségük az adatok forgalmazásához. Az olyan eszközök, melyek közvetlenül kapcsolódnak egymáshoz, és ugyanazon érintkezőket használják adásra és vételre, azonos jelkiosztással csatlakozó eszközöknek nevezzük. Keresztkötésű kábelre van szükségük az adattovábbítás érdekében.

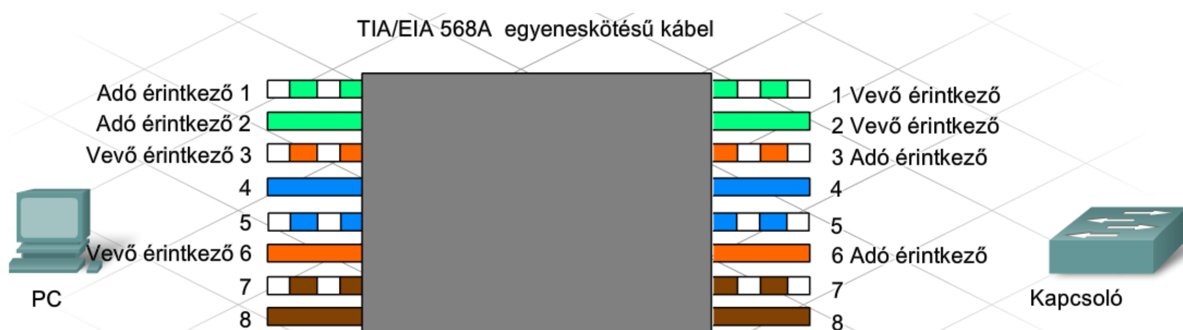
Ellentétes jelkiosztással csatlakozó eszközök

Egy személyi számítógép RJ-45-ös csatlakozóján az 1-2 érintkezők felelnek a küldésért, a 3-as és a 6-os a fogadásért. Egy kapcsoló hálózati csatlakozóján az 1-2-es érintkezők fogadnak, a 3-as és a 6-os érintkezők küldenek. A számítógépnél küldésre használt érintkezők, a kapcsoló esetén fogadásra használtak. Így egyeneskötésű kábelre van szükség.

A kábel egyik végén, a számítógép 1-es érintkezőjére kötött vezeték (adó érintkező) össze van kötve a kapcsoló 1-es érintkezőjével (vevő érintkező).

Másik példák, melynél a Ellentétes jelkiosztássalos csatlakozó eszközök egyeneskötésű kábelt igényelnek:

- Kapcsoló - Forgalomirányító
- Hub - Személyi számítógép



Azonos jelkiosztásos csatlakozójú eszközöknek

Ha egy számítógép közvetlenül csatlakozik egy másik számítógéphez, mindkét eszköznél az 1-2-es érintkezőket küldésre, míg a 3-as és a 6-os érintkezőket vételre használják.

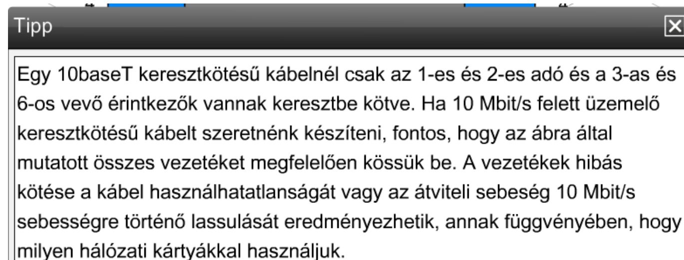
Egy keresztkötésű kábel biztosítja azt, hogy az egyik számítógép 1-es és 2-es érintkezőire (adó érintkezők) kötött zöld vezeték a másik számítógép 3-as és 6-os érintkezőihez (vevő érintkezők) kapcsolódjon.

Ha egyeneskötésű kábelt használnánk, a PC1 1-es adó érintkezőjére kötött vezeték a PC2 1-es adó érintkezőjével lenne összekötve. Nem lehetséges egy adó érintkezőn információt fogadni.

Egyéb példák hasonló eszközökre, melyek keresztkötésű kábelt igényelnek:

- Kapcsoló port - Kapcsoló port
- Kapcsoló port - hub port
- Hub port - hub port
- Forgalomirányító port - forgalomirányító port
- PC - forgalomirányító port
- PC - PC

Ha helytelen típusú kábelt használunk, a két hálózati eszköz közötti kapcsolat nem lesz működőképes.



Némely eszköz képes automatikusan érzékelni, mely érintkezőket kell adásra és vételre használni, ennek megfelelően állítják be belső áramköreiket.



4.5.3 UTP kábelek végződése

AZ UTP és STP kábeleket rendszerint RJ-45-ös csatlakozókkal látják el.

Az RJ-45-ös csatlakozó egy olyan "apa" csatlakozó, melyet a kábel végére kell krimpelni (préselni). Amikor ezt a csatlakozót a fém érintkezőivel felfelé nézzük, látható, hogy az érintkezők helyei balról jobbra 8-tól 1-ig vannak számozva.

Az aljzat a csatlakozás "anya" résztvevője, és a hálózati eszközökön, fali kimeneteken, vagy patch paneleken található meg. A vezeték RJ-45-ös csatlakozóját az aljzatba kell dugni.

Forgalomban vannak olyan kábelek, melyekre gyárilag fel vannak szerelve az RJ-45-ös csatlakozók. Ezenkívül, a helyszínen magunk is elvégezhetjük a kábelek lezárását , egy krimpelő fogót használva. Mikor RJ-45-ös csatlakozót akarunk felhelyezni egy UTP kábelre, csak rövid kábelrészt csavarjunk szét, ezzel is minimalizálva az áthallást. Valamint győződjünk meg arról, hogy a vezetékek teljesen be vannak tolva a csatlakozó végébe, és az RJ-45-ös csatlakozót a kábel burkolatára préseltük. Ez a csatlakozás jó elektromos összeköttetést és stabil rögzítési lehetőséget biztosít.

4.5.4 UTP kábelek végződése Patch panelekbe és fali ajzatokba

Egy hálózati központban a hálózati eszközöket általában patch panelekhez csatlakoztatják. A patch panelek kapcsolótáblaként funkcionálnak, összekötve a munkaállomások kábeleit a többi hálózati eszközzel. A patch panelek használata lehetővé teszi a fizikai kábelezés gyors áthelyezhetőségét a hálózati eszközök hozzáadása vagy áthelyezése esetén. Ezek a panelek az előlapjukon RJ-45-ös csatlakozókat használnak a gyors csatlakoztathatóság végett, de ehhez az RJ-45 aljzat hátulján, a kábelek betűzése szükséges.
Manapság patch paneleket már nem csak nagyvállalati hálózatoknál használnak. Megtaláljuk őket számos kisvállalati környezetben, vagy akár otthonokban is, ahol központi kapcsolódási pontot nyújtanak az adat és telefonos hálózatok, valamint hangrendszerek esetén.

Az RJ-45-ös csatlakozó 8 érintkezővel rendelkezik, és a T568A vagy T568B séma szerint kell bekötni. A patch panel szerelésekor egy eszköz szükséges, melyet betűző szerszámként (punchdown tool) ismerünk, a vezetékek csatlakozóba való préseléséhez. Az egyes vezetékeket színük szerint helyezzük a megfelelő önblankoló csatlakozóhoz (IDC), mielőtt betűzzük őket. A betűző szerszám levágja a felesleges kábeldarabot is.

A legtöbb fali csatlakozó szerelése nem igényel betűző eszközt. Az ilyen típusú aljzatok szerelésekor a kábeleket szét kell csavarni egymástól, és a megfelelő IDC fölé kell helyezni. A csatlakozókra ráhelyezett fedél benyomja a kábelt az IDC-be, és átvágja a vezeték szigetelését. Ebben az esetben a szakember feladata a felesleges kábeldarabok eltávolítása.

Minden esetben, az érpároknak a szükségesnél hosszabb szétcsavarása, növeli az áthallás mértékét, és csökkenti az egész hálózat teljesítményét.

4.5.5 A kábelek tesztelése

Amikor egy új vagy javított kábelt szerelünk, nagyon fontos meggyőződni arról, hogy a kábel megfelelően működik, és megfelel az összekapcsolhatósági szabványoknak. Ezekről különböző tesztek elvégzésével győződhetünk meg.

Az első teszt a vizuális vizsgálat, mely által meggyőződünk arról, hogy minden vezeték a T568A vagy B szerint van összekötve.

Valamint ellenőrizzük elektronikusan is a kábelt, a szerelvény hibáinak vagy sérüléseinek kiderítéséhez. A következő eszközöket használhatjuk kábelek vizsgálatához:

- Kábel tesztelők
- Kábel hitelesítők
- Multiméterek

Kábelteszter

A kábelteszter a kábelek különböző hibáinak kiszűrését teszi lehetővé, mint például a rövidzár vagy a szakadás, illetve a rossz színsorrendű bekötés.

Kábelminősítő műszer

A kábelminősítő műszer meghatározza a kábel pontos teljesítőképességét, majd grafikus formában jeleníti meg a felhasználónak.

Multiméter

Multiméterrel mérhető az egyen- és váltakozó áram feszültsége, erőssége és más elektromos- illetve kábeljellemzők.

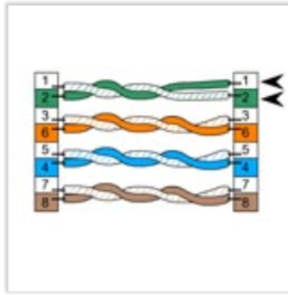
A kábeltesztereket kezdeti kábelvizsgálatokhoz használják. Az első tesztet általában folytonossági vizsgálatnak hívják, amely igazolja a végponttól-végpontig terjedő kapcsolódást. Képes a gyakori kábelezési hibák felismerésére is, mint például, a szakadások (nyitott áramkör) és rövidzárak.

Egy áramkör akkor nyitott, amikor egy vezeték nem megfelelően van belenyomva a csatlakozóba és nincs elektromos érintkezés. Szakadás akkor is létrejöhet, ha vezetékben törés következett be.

Rövidzárlat akkor áll elő, ha a réz vezetők érintkeznek egymással. Miképp az elektromos impulzus végighalad a vezetéken, egy másik érintkező vezeték kerül az útjába. Ez a jelenség egy nem tervezett útvonalat hoz létre a jel terjedésében.

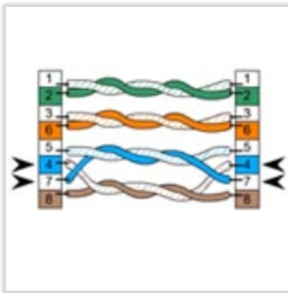
Egy kábelteszter képes vezeték térképek létrehozására, mellyel megállapítható a kábel megfelelő érintkezése. A vezetéktérkép megmutatja, melyik érpár melyik érintkezőkhöz csatlakozik a csatlakozón és az aljzaton. A vezeték térkép teszt bizonyítja, hogy minden vezeték a megfelelő érintkezőre van kötve, és jelzi, ha kábelezési hibák merültek fel, úgymint osztott vagy felcserélt érpárak.

Ha ezek közül bármelyik előfordul, a legegyszerűbb, ha újraszereljük a kábelvég csatlakozóit.



Felcserélt érpárak

A felcserélt érpárak problémáról akkor beszélünk, ha egy érpárat megfelelően szereltek a kábel egyik végén, de felcserélve használták őket a másik oldalon. Például, ha a kábel egyik végén a zöld/fehér vezetéket kötjük az 1-es érintkezőre és a zöldet a 2-esre, a másik végen pedig felcseréljük őket, akkor ez a kábel felcserélt érpárak hibáját okozza.



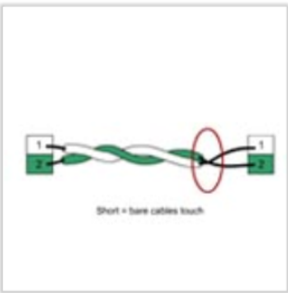
Osztott érpárak

Az osztott érpárak hiba akkor következik be, ha a kábel mindkét végén, egy pár egyik vezetékét felcseréljük egy másik pár vezetékével. Gondosan vizsgáljuk meg az ábrán látható érintkező sorszámokat, így észre fogjuk venni a bekötési hibát. Az érpárok felcserélésével két küldő vagy fogadó érpár jön létre, mindegyik olyan vezetékekből áll, amelyek nincsenek összecsavarva egymással. A csere miatt megszűnik a kölcsönös kioltási hatás, és a kábel érzékenyebbé válik az áthallásra és az interferenciára.



Nyitott

Hiba a huzalozásban, melyet az áramkör folytonosságának szakadása okoz.



Rövidzárlat

Rövidzárlat akkor következik be, ha két vezeték réz felületei érintik egymást.

A speciális kábelteszterek további információkat képesek szolgáltatni, például a csillapítás és az áthallás szintje.

Csillapítás

A csillapítást gyakran nevezik beiktatási veszteségnek, ami egy általános fogalom, és a jel erősségének csökkenését jelenti. A csillapítás természetes következménye bármely közegen történő jelátvitelnek. A csillapítás korlátozza a hálózati kábel hosszát, melyen még küldhetők az üzenetek. Egy kábel teszter úgy méri a csillapítást, hogy jelet küld a kábel egyik végéről, és megméri a jel erősségét a kábel másik végén.

Áthallás

Az áthallás az érpárak közötti jelek szivárgását jelenti. Ha ezt a jel adásához közeli helyen mérik, akkor közelvégi áthallásról beszélünk (NEXT). Ha a kábel fogadó oldalán mérik ezt az értéket, akkor távolvégi áthallásnak (FEXT) nevezzük. Az áthallás mindkét formája csökkenti a hálózati teljesítményt, és gyakran az okozza, hogy túl hosszan csavarták szét a kábelt a csatlakozók szerelésénél. Ha magas áthallási értékeket mértünk, a legjobb dolog, amit tehetünk, hogy ellenőrizzük a kábelcsatlakozókat, és újraszereljük őket, ha szükséges.

4.5.6 Hasznos kábelezési tanácsok

A következő hasznos kábelezési lépések segítségével megbizonyosodhatunk afelől, hogy sikeresen végződtetjük a kábelt.

1. Nagyon fontos, hogy a hálózatban használt kábeltípusok és összetevők, következetesen megfeleljenek a hálózatban használandó szabványoknak. A korszerű konvergált hálózatok képesek egyazon vezetéken hang, videó és adat alapú információkat forgalmazni; így a konvergált hálózatokban használt kábeleknek támogatniuk kell ezen felhasználási területeket.
2. A kábelszabányok meghatározzák a különböző kábelek maximális hosszúságát. Mindig ragaszkodjunk a hosszúság-korlátozásokhoz az adott kábeltípus használata esetén.
3. Az UTP is, mint minden réz alapú kábel, érzékeny az elektromágneses interferenciára (EMI). Nagyon fontos, hogy a különböző interferencia forrásoktól, úgymint a nagyfeszültségű vezetékektől és fluoreszkáló világításoktól, távol telepítsünk ilyen kábeleket. A televíziók, számítógépes monitorok és mikrohullámú sütők ugyancsak jó példák egyéb interferencia-forrásokra. Néhány esetben szükség van arra, hogy az adatkábeleket egy külön vezetőcsőben telepítsük, megvédve így az EMI és RFI zavaroktól.
4. A helytelen kivégződtetések, rossz minőségű kábelek és csatlakozók használata okozhatja a kábel adatátviteli kapacitásának csökkenését. Mindig kövessük a kábelek lezárására vonatkozó szabályokat, és teszteléssel ellenőrizzük, hogy a lezárás megfelelő.
   5. Teszteljünk le minden kábel szerelvényt a megfelelő csatlakozások és működés érdekében.
5. Minden kábelt címkézzünk fel, amint azokat lefektettük, és jegyezzük le a kábelek helyét a hálózat dokumentációjában.

A strukturált kábelezés egy olyan eljárás, mely egy szervezett kábelezési rendszert hoz létre, ez könnyen megérthető a hálózati telepítők, rendszergazdák és bármely más kábelekkel foglalkozó szakemberek számára. A strukturált kábelezés egyik összetevője a kábelmenedzsment.

A kábelmenedzsment többféle feladatot lát el. Először is rendezett és szervezett rendszert biztosít, mely segít elkülöníteni a kábelek esetleges problémáit. Másod sorban, a kábelmenedzsment által előírt lépéseket követve, a kábelek védettek lesznek a fizikai sérülésektől, ami nagyban csökkenti a tapasztalható problémák számát.

A kábeleket hosszú távú befektetésként kell kezelni. De, ami ma elegendő, a jövőben már nem biztos, hogy az lesz. Mindig vegyük számításba a jövő igényeit, a jelen szabványok betartásával. Emlékezzünk arra, hogy szabványok segítenek abban, hogy a technológia fejlődése során, a kábelek képesek legyenek elfogadható teljesítményt nyújtani.

Minden környezetben nagyon fontos a hasznos kábelezési tanácsok betartása. Szorosan ragaszkodjunk ezekhez a módszerekhez, az otthoni és kisvállalati hálózatoknál is, így csökkentve a lehetséges problémák előfordulását. Sok időt, pénzt és idegességet spórolhatunk meg betartásukkal.

4.6 Összefoglalás

Ez a fejezet bemutatja az Internetet, mint számítógépes hálózatok világméretű gyűjteményét, melyek közös szabványokat használva működnek együtt az információk cseréjéhez. Az Internet hozzáférés érdekében csatlakozni kell egy Internetszolgáltatóhoz (ISP).

- Egy ISP olyan vállalat, mely kapcsolatokat nyújt és támogatást biztosít az Internethez.
- Az ISPk kis- és nagyméretű földrajzi területeket is ellátnak.
- Olyan szolgáltatásokat nyújtanak, mint elektronikus levelezés, webkiszolgálás, IP telefónia és DNS szolgáltatás.
- A különálló számítógépek és helyi hálózatok a szolgáltatás-elérési ponton (POP) csatlakoznak az ISP-hez.
- Az ISP-hez kapcsolódhatunk betárcsázós, DSL, Kábeles, vezeték nélküli vagy műholdas kapcsolaton keresztül.

- Az Internet legfontosabb protokollja az Internet Protokoll (IP).
- Az Internet protokoll csomagokra tördeli az adatokat, melyek 500 - 1500 byte méretűek lehetnek és érvényes forrás és cél IP-címmel kell rendelkezniük.
- Az IP-címeknek egyedinek kell lenniük az Interneten.
- Minden ISP rendelkezik egy hálózati-vezérlő létesítménnyel, ezt Hálózatüzemeltető Központnak (NOC) nevezünk, amely vezérli a hálózati forgalmat, és helyet ad a különböző kiszolgálóknak, mint a levelezőkiszolgáló és webkiszolgáló.
- A ping és tracert olyan segédprogramok, melyekkel tesztelhető az eszközök között kapcsolat.

- A hálózati diagramokon a felhő ábra általában az Internetet jelképezi, a kapcsolatok részletezése nélkül.
- Az Internet felhőben forgalomirányítókat használnak a cél és forrás közötti különböző útvonalak biztosításához.
- Az ISP-k elfogadják és kézbesítik a végfelhasználók és más Internetszolgáltatók információit, számos technológia felhasználásával.
- Az Internetszolgáltatóknál megtalálható hálózati eszközök korszerűek és nagysebességűek, valamint hibatűrési lehetőséggel (redundancia) is rendelkeznek.
- Egy szolgáltatónak számolnia kell a hálózati eszközök és kiszolgálók fizikai szükségleteivel, úgymint energiaellátás és légkondicionálás.

A kommunikáció végbemeneteléhez valamilyen átviteli közegnek jelen kell lennie a jelek hordozása végett. A hálózatok világában az átviteli közeg általában fizikai kábelezés:

- A hálózati kábeleket két nagy csoportra oszthatjuk: réz alapú kábelek, melyek elektromos impulzusokat szállítanak, és az üvegszálas kábelek, melyek fényhullámokat használnak.
- A réz kábelezés, például UTP és koaxiális kábel, nagyon érzékeny mind az elektromágneses (EMI), mind a rádiófrekvenciás (RFI) interferenciára. Az üvegből vagy műanyagból készült optikai kábelek immunisak az EMI és RFI zavarokra.
- Az árnyékolatlan csavart érpáras (UTP) kábeleket használják a legtöbb Ethernet hálózatban.
- A koaxiális kábeleket gyakran használják kábeltelevíziós és Internetes kapcsolatokhoz, nagy sávszélességgel rendelkeznek, mely lehetővé teszi több jel kombinálását vagy multiplexelését.
- Az üvegszálas kábelek hatalmas sávszélességgel bírnak és alkalmasak gerinchálózati kábelezésre.

- A kábelezési szabványok útmutatást adnak a kábelek telepítéséhez és teszteléséhez, hogy a technológia fejlődésével biztosítsák az elfogadható teljesítményt.
- TIA/EIA csavart érpáras bekötési sémák a T568A és T568B.
- A különböző kábeltípusok különböző bekötési sémákkal rendelkeznek. Gyakori UTP kábeltípusok az egyeneskötésű, keresztkötésű és rollover (konzol) kábelek.
- A kábelteszterek ellenőrzik a kábelek folytonosságát, hibás csatlakozásait, osztott és felcserélt érpárjait. Egy kábelteszter képes megmérni a vezeték csillapítását és áthallását.
- A hasznos kábelezési tanácsok segítenek az előforduló kábelezési hibák és problémák számának csökkentésében, valamint alkalmazásukkal sok időt, pénzt és fáradságot takaríthatunk meg.

5. Hálózati címzés

5.1 IP címek és alhálózati maszkok

5.1.1 Az IP címek célja

Egy állomásnak IP-címre van szüksége, hogy része lehessen az Internetnek. Az IP-cím egy logikai hálózati cím, ami azonosít egy bizonyos állomást. Megfelelően kell konfigurálni és egyedinek kell lennie ahhoz, hogy kommunikálni tudjunk más eszközökkel az Interneten.

Az IP címet az állomás hálózati csatolóeszközének kapcsolatához rendelik. Ez a kapcsolat általában egy hálózati csatoló (NIC), ami az eszközbe van szerelve. A hálózati illesztővel rendelkező végfelhasználói eszközökre példák a munkaállomások, kiszolgálók, hálózati nyomtatók és IP-telefonok. Némely kiszolgálónak egynél több hálózati csatolója lehet, és ezek mindegyike saját IP címmel rendelkezik. A forgalomirányító interfészei, amelyek a kapcsolatot biztosítják egy IP hálózathoz, szintén rendelkeznek IP címmel.

Minden, az Interneten keresztül küldött csomagnak van egy forrás és egy cél IP címe. Ezt az információt igénylik a hálózati eszközök, hogy biztosítsák az információ eljutását a célhoz, és bármely válasz visszatérését a forráshoz.

5.1.2 Az IP címek felépítése

Egy IP cím nem más, mint 32 bináris számjegy (nullák és egyesek) sorozata. Az emberek számára nagyon nehéz egy bináris IP cím kiolvasása. Emiatt a 32 bitet négy, 8 bitből álló bájtba csoportosítják, amit oktettnek hívunk. Egy IP cím ebben a formában az emberek számára nehezen olvasható, írható és memorizálható. Azért, hogy egy IP címet könnyebben megérthessünk, minden oktettet a decimális megfelelőjével írunk le, és egy decimális pont karakterrel választunk el. Ezt úgy hívjuk, hogy decimális, pontozott jelölés.

Amikor egy állomásnak beállítjuk az IP címét, akkor azt pontozott decimális számként adjuk meg, mint például 192.168.1.5. Képzeljük el, ha a 32 bites bináris megfelelőjét kéne bevinnünk, ami 11000000101010000000000100000101. Ha csak egyetlen bitet elgépelünk, a cím már más lenne, és az állomás nem lenne képes kommunikálni a hálózaton.

A 32 bites IP címet az IP 4-es verziója, az IPv4 írja le, és jelenleg a leggyakoribb IP címforma az Interneten. Több mint 4 milliárd lehetséges IP cím létezik a 32 bites címzési séma felhasználásával.

Amikor egy állomás fogad egy IP címet, megvizsgálja mind a 32 bitet, ahogy azt megkapta a NIC-től. Az embereknek viszont át kell alakítaniuk ezt a 32 bitet a négy oktettes decimális megfelelőjére. Minden oktett 8 bitből áll, és minden bitnek van helyiértéke. A 8 bit négy csoportján belül ugyanazok a helyiértékek. A jobb oldali szélső bitnek 1 a helyiértéke, a maradék biteknek pedig jobbról balra 2, 4, 8, 16, 32, 64 és 128.

Az oktett értékét úgy állapítjuk meg, hogy összeadjuk a helyiértékeket azokban a pozíciókban, ahol bináris 1 van.

- Ha 0 szerepel egy pozíción, akkor nem adjuk hozzá a helyiértéket.



- Ha mind a 8 bit nulla. 00000000 az oktett értéke 0.
- Ha mind a 8 bit 1-es, 11111111, akkor az oktett értéke 255 (128+64+32+16+8+4+2+1).
- Ha a 8 bit kevert, mint például 00100111, akkor az oktett értéke 39 (32+4+2+1).

Tehát a négy oktett mindegyikének értéke 0 és a maximális 255 közé esik.

5.1.3 Az IP cím részei

A logikai 32 bites IP cím hierarchikus, és két részből áll. Az első rész azonosítja a hálózatot, a második rész pedig egy állomást azon a hálózaton. Mindkét részre szükség van az IP címben.

Például, ha az állomásnak 192.168.18.57 az IP címe, akkor az első három oktett (192.168.18) azonosítja a cím hálózati részét, és az utolsó oktett (57) azonosítja az állomást. Ez hierarchikus címzésként ismert, mivel a hálózati rész jelöli a hálózatot, amin minden egyes egyedi állomáscím elhelyezkedik. A forgalomirányítóknak csak azt kell tudni, hogyan érik el az egyes hálózatokat, ahelyett, hogy ismernék minden egyes különálló gép helyét.

Másik példa a hierarchikus hálózatra a telefonrendszer. Egy telefonszám, az országkód, a körzetszám és központszám jelenti a hálózati címet, a maradék számjegyek pedig a helyi telefonszámot.

5.1.4 Hogyan működnek együtt az IP címek és az alhálózati maszkok

Minden IP cím két részből áll. Honnan tudják az állomások, melyik a hálózatcím, és melyik az állomáscím? Ennek kijelölése az alhálózati maszk feladata.

Amikor egy IP állomást beállítunk, egy alhálózati maszkot is rendelünk az IP cím mellé. Ahogy az IP cím, az alhálózati maszk is 32 bit hosszú. Az alhálózati maszk jelöli ki, hogy az IP cím melyik része a hálózatcím és melyik az állomáscím.

Az alhálózati maszkot összehasonlítjuk az IP címmel balról jobbra, bitről bitre. Az egyesek az alhálózati maszkban a hálózati részt jelentik; a nullák jelentik az állomás részt. A bemutatott példában az első három oktett a hálózat, és az utolsó oktett jelöli az állomást.

Amikor egy állomás csomagot küld, az alhálózati maszk alapján összehasonlítja a saját és a cél IP cím hálózatcím részét. Ha a hálózati bitek egyeznek, akkor mind a forrás, mind a cél azonos hálózaton van, a csomag helyileg kézbesíthető. Ha nem egyeznek, a küldő állomás a helyi forgalomirányító interfészéhez továbbítja a csomagot, hogy az továbbküldje a másik hálózatra.

Az otthoni és kis üzleti hálózatokban leggyakrabban a következő alhálózati maszkokat látjuk: 255.0.0.0 (8 bit), 255.255.0.0 (16 bit) és 255.255.255.0 (24 bit). A 255.255.255.0 (decimális) vagy 11111111.11111111.1111111.00000000 (bináris) formájú alhálózati maszk 24 bitet használ arra, hogy azonosítsa a hálózatot, így 8 bit marad a hálózat állomásainak azonositására.

A hálózaton elhelyezhető állomások maximális számának kiszámításához vegyük a 2-es számot annyiadik hatványon, amennyi az állomásbitek száma (2^8 = 256). Ebből a számból ki kell vonnunk kettőt (256-2). A kivonás oka az, hogy a csupa 1-esekből álló állomásazonosító rész ennek a hálózatnak az üzenetszórási címe, ezért nem rendelhető állomáshoz. A csupa 0-ból álló állomásazonosító a hálózat-azonosítót jelenti, és ismét nem rendelhető állomáshoz. A 2 hatványai a Windows operációs rendszerek részét képező kalkulátorral könnyen kiszámíthatók.

Egy másik mód az állomások számának kiszámítására az, hogy összeadjuk a rendelkezésre álló állomásbitek helyiértékeit (128+64+32+16+8+4+2+1 = 255). Ebből a számból vonjunk ki egyet (255-1=254), mert minden állomásbit nem lehet 1-es. Nem szükséges 2-t kivonni, mert az összes 0-ás bit értéke nulla, és ez nem szerepel az összeadásban.

Egy 16 bites maszkkal 16 bit (két oktett) az állomásoké, és egy állomáscím lehet csupa 1-es valamelyik oktettben. Ez úgy nézhet ki, mint egy üzenetszórási cím, de mivel a másik oktett nem csupa 1-es, ezért ez egy érvényes állomáscím. Emlékezzünk vissza, hogy az állomás az összes állomásbitet együtt nézi, nem az oktett értékeket.

5.2 Az IP címek típusai

5.2.1 Az IP címosztályok és az alapértelmezett alhálózati maszkok

Az IP cím és az alhálózati maszk együttműködik azért, hogy meghatározzák, az IP cím melyik része jeleníti meg a hálózat címét, és melyik az állomások címét.

Az IP címeket 5 osztályba soroljuk. Az A, B és C osztályok üzleti felhasználású címek és állomásokhoz rendeljük őket. A D osztályt a csoportos címzéshez foglalták le, míg az E osztályt kísérleti célokra.

A C osztályú címeknek három oktettje van a hálózatok részére és egy az állomásoknak. Az alapértelmezett alhálózati maszk 24 bites (255.255.255.0). A C osztályú címeket általában kisebb hálózatokhoz rendelik.

A B osztályú címekben két oktett jeleníti meg a hálózati részt és kettő az állomásazonosítót. Az alapértelmezett alhálózati maszk 16 bites (255.255.0.0). Ezeket a címeket tipikusan a közepes méretű hálózatokban használják.

Az A osztályú címeknek csak egy oktettje jeleníti meg a hálózati részt, és három reprezentálja az állomásokat. Az alapértelmezett alhálózati maszk 8 bites (255.0.0.0). Ezeket a címeket jellemzően nagy szervezetekhez rendelik hozzá.

A cím osztálya megállapítható az első oktett értékéből. Például, ha az IP cím első oktettjének értéke a 192-223 tartományba esik, akkor a C osztályba soroljuk. Például, a 200.14.194.67 egy C osztályú cím.

IP-címosztályok

Címosztály	Első oktett tartomány (decimális)	Az első oktett bitek (a zöld bitek nem változnak)	Egy cím hálózati (N) és állomás (H) részei	Alapértelmezett alhálózati maszk (decimális és bináris)	A lehetséges hálózatok és hálózatonkénti állomások száma
A	1 - 127	00000000 - 01111111	N.H.H.H	255.0.0.0 11111111.00000000.00000000.00000000	126 hálózat (2^7-2) 16777214 állomás hálózatonként (2^24-2)
B	128 - 191	10000000 - 10111111	N.N.H.H	255.255.0.0 11111111.11111111.00000000.00000000	16382 hálózat (2^14-2) 65534 állomás hálózatonként (2^16-2)
C	192 - 223	11000000 - 11011111	N.N.N.H	255.255.255.0 11111111.11111111.11111111.00000000	2097150 hálózat (2^21-2) 254 állomás hálózatonként (2^8-2)
D	224 - 239	11100000 - 11101111	Nem használható üzleti célra mint állomás		
E	240 - 255	11110000 - 11111111	Nem használható üzleti célra mint állomás		

^^ A csupa nullás (0) és csupa egyes (1) nem érvényes állomáscím.

5.2.2 Nyilvános és magán IP címek

Minden állomásnak, amely közvetlenül csatlakozik az Internetre, egyedi nyilvános IP címre van szüksége. A 32 bites címek véges száma miatt megvan a veszélye annak, hogy kifogyunk az IP címekből. E probléma egyik megoldásaként kizárólagosan csak szervezeten belüli (privát) használatra lefoglalták az IP címek egy csoportját. Ezzel lehetővé válik hogy a szervezeten belüli állomások anélkül kommunikáljanak egymással, hogy egyedi nyilvános IP címeket használjanak.

Az RFC 1918 egy szabvány, ami mindhárom (A, B és C) osztályon belül lefoglal néhány címtartományt. Ahogy a táblázatban látható, ezek a magán címtartományok egy A osztályú, 16 B osztályú és 256 C osztályú hálózatot tartalmaznak. Ez meglehetős rugalmasságot ad a hálózati adminisztrátornak a belső címek kiosztásában.

Egy nagyon nagyméretű hálózat használhatja az A osztályú magánhálózatot, ami több mint 16 millió magáncímet enged meg.

A közepes méretű hálózatokon a B osztályú magánhálózatot használhatjuk, ami 65000 címet biztosít.

Az otthoni és kisméretű üzleti hálózatok jellemzően egy C osztályú magáncímet használnak, ami legfeljebb 254 állomást enged meg.

Az A osztályú hálózat, a 16 B osztályú hálózat vagy a 256 C osztályú hálózat használható bármely méretű szervezeten belül. Sok szervezet jellemzően az A osztályú magánhálózatot használja.

Címosztály	A lefoglalt hálózatazonosítók száma	Hálózatcímek
A	1	10.0.0.0
B	16	172.16.0.0 - 172.31.0.0
C	256	192.168.0.0 - 192.168.255.0

A magáncímeket az állomások a szervezeten belül mindaddig használhatják, amíg nem kapcsolódnak közvetlenül az Internetre. Ezért ugyanazt a magán címtartományt több szervezet is használhatja. A magáncímeket nem irányítják az Interneten és gyorsan blokkolja őket a szolgáltató forgalomirányítója.

A magáncímek használata bizonyos mértékű biztonságot is ad, mivel ezek csak a helyi hálózaton látszanak, és a kívülállók nem kapnak közvetlen hozzáférést a magán IP címekhez.

Vannak olyan magáncímek is, amiket az eszközök diagnosztikai tesztelésére használhatunk. Ezt a típusú magáncímet visszahurkolási címként ismerjük. Az A osztályú 127.0.0.0 hálózatot a visszahurkolási címekhez foglalták le.

5.2.3 Egyedi, üzenetszórásos és csoportos címzés

A címosztályokon kívül az IP címeket egyedi, üzenetszórásos vagy csoportos címzésű kategóriákba is soroljuk. Az állomások az IP címeket használhatják egy-az-egyhez (egyedi), egy-a-többhöz (csoportos címzés) és egy-mindenkihez (üzenetszórásos) típusú kommunikációra.

Egyedi címzés

Az egyedi cím a leggyakoribb típus egy IP hálózaton. Egy egyedi célcímmel ellátott csomag egy megadott állomásnak szól. Példaként vegyük a 192.168.1.5-ös IP címmel rendelkező állomást (forrás), ami lekér egy weboldalt a 192.168.1.200-as IP címmel rendelkező kiszolgálótól (cél).

Ahhoz, hogy egyedi címzésű csomagot küldhessünk és fogadhassunk, a cél IP címnek szerepelnie kell az IP csomag fejrészében. A megfelelő cél MAC-címnek szintén benne kell lennie az Ethernet keret fejrészében. Az IP-cím és a MAC-cím együttesen kézbesíti az adatokat egy adott célállomáshoz.

Szórás

Üzenetszóráskor a csomag olyan cél IP címet tartalmaz, aminél csupa 1-es áll az állomásazonosítónál. Ez azt jelenti, hogy a helyi hálózat összes állomása (szórási tartomány) megkapja és megvizsgálja a csomagot. Sok hálózati protokoll, mint például az ARP és a DHCP üzenetszórást használ.

A C osztályú 192.168.1.0 hálózatnak, az alapértelmezett 255.255.255.0 alhálózati maszkkal, 192.168.1.255 az üzenetszórási címe. Az állomásazonosító rész a decimális 255 vagy bináris 11111111 (minden 1-es).

A B osztályú 172.16.0.0 hálózat, az alapértelmezett 255.255.0.0 alhálózati maszkkal, a 172.16.255.255 szórási címmel rendelkezik.



Az A osztályú 10.0.0.0 hálózatnak - az alapértelmezett 255.0.0.0 alhálózati maszkkal - 10.255.255.255 szórási címe van.

A hálózat üzenetszórási IP címének van egy megfelelő MAC szórási címe is az Ethernet keretben. Az Ethernet hálózatokon a MAC szórási cím 48 darab egyes, hexadecimálisan megjelenítve FF-FF-FF-FF-FF-FF.

Csoportos küldés

A csoportos címek lehetővé teszik a forráseszköz számára, hogy eszközök egy csoportjának küldjön csomagot.

Azoknak az eszközöknek, amik többes címzésű csoporthoz tartoznak, csoportos IP címe van. A csoportos címek tartománya 224.0.0.0-tól 239.255.255.255-ig terjed. Mivel a csoportos címek a címek egy csoportját jelentik (néha úgy nevezik, hogy állomáscsoport), ezeket csak a csomag céljaként használhatjuk. A forrásnak mindig egyedi címe van.

A csoportos címzésre példaként említhetjük a távoli játékokat, ahol sok játékos kapcsolódik össze távolról, de ugyanazt a játékot játszák. Másik példa lehet a távoktatás videokonferencia segítségével, ahol több tanuló kapcsolódik ugyanahhoz az osztályhoz.

Ugyanúgy, mint az egyedi vagy szórási címeknek, a csoportos címeknek is szüksége van egy megfelelő csoportos MAC címre, hogy kézbesíteni tudják a kereteket a helyi hálózaton. A csoportos MAC cím egy speciális érték, ami hexadecimális 01-00-5E-vel kezdődik. A vége pedig a csoportos IP cím alsó 23 bitjének átalakításával áll elő, amit az Ethernet cím maradék 6 hexadecimális karakterévé kódolunk át. Például, mint az ábrán is látható, a hexadecimális 01-00-5E-0F-64-C5. Minden hexadecimális karakter 4 bináris bit.

5.3 Hogyan szerezhetők meg az IP címek

5.3.1 Statikus és dinamikus címhozzárendelés

Az IP címek statikusan és dinamikusan is hozzárendelhetők.

Statikus

A statikus hozzárendelésnél a hálózati rendszergazdának kézzel kell beállítania a hálózati információkat az állomáson. Minimálisan ez az IP címet, alhálózati maszkot és az alapértelmezett átjárót tartalmazza.

A statikus címeknek van néhány előnye. Például hasznosak a nyomtatók, kiszolgálók és más hálózati eszközök számára, amelyeknek elérhetőnek kell lennie a hálózaton az ügyfelek számára. Ha az állomások alapesetben a kiszolgálót egy adott IP címen érik el, akkor nem jó, ha az a cím megváltozik.

A címinformációk statikus hozzárendelése a hálózati erőforrások fölött megnövelt ellenőrzést adhat, de időigényes lehet minden állomáson beállítani az információkat. Amikor az IP címet statikusan visszük be, az állomás csak alapvető hibaellenőrzést végez rajta. Emiatt nagyobb valószínűséggel fordulnak elő hibák.

Amikor statikus IP címzést használunk, fontos, hogy karbantartsunk egy pontos listát arról, hogy melyik IP címet melyik eszközhöz rendeltük. Ezen kívül, ezek állandó címek és alapesetben nem használhatók fel újra.

Dinamikus

A helyi hálózatokon gyakori eset, hogy a felhasználók száma gyakran változik. Új felhasználók érkeznek laptoppal, és kapcsolódni szeretnének. Másoknak új munkaállomásaik vannak, amiket csatlakoztatni kell. Ahelyett, hogy a rendszergazda rendelne ki minden állomásnak egy IP címet, könnyebb, ha ezeket automatikusan osztjuk ki. Ezt egy dinamikus állomáskonfiguráló protokollnak (Dynamic Host Configuration Protocol, DHCP) nevezett protokollal oldjuk meg.

A DHCP lehetőséget biztosít a címzési információk automatikus hozzárendelésére, úgymint IP cím, alhálózati maszk, alapértelmezett átjáró és egyéb beállítási információk.

A DHCP általában előnyben részesített módszer az állomások IP cím hozzárendeléséhez a nagy hálózatokon, mivel csökkenti a hálózati kiszolgáló-személyzet terheit és látszólagosan kizárja a beviteli hibákat.

A DHCP másik előnye, hogy egy címet nem állandó használatra, hanem csak egy időtartamra bérelnek ki az állomások. Ha az állomást kikapcsolják vagy eltávolítják a hálózatról, a cím visszatér a készletbe újrafelhasználásra. Ez különösen a mobil felhasználóknál hasznos, akik jönnek és mennek a hálózaton.

5.3.2 DHCP kiszolgálók

Ha belépünk egy vezeték nélküli csatlakozási pontra (hotspot) egy repülőtéren vagy kávézóban, a DHCP lehetővé teszi számunkra az Internet-elérést. Amint belépünk a területre, a laptopunk DHCP ügyfele kapcsolódik a helyi DHCP kiszolgálóhoz vezeték nélküli kapcsolat segítségével. A DHCP kiszolgáló kioszt egy IP címet a laptopnak.

Különböző típusú eszközök lehetnek DHCP kiszolgálók, ha DHCP szolgáltató programot futtatnak. A legtöbb közepes és nagyméretű hálózatban a DHCP kiszolgáló általában egy erre a célra kinevezett PC-alapú kiszolgáló.

Az otthoni hálózatoknál a DHCP kiszolgáló általában az Internet-szolgáltatónál (ISP) helyezkedik el, és az otthoni hálózaton lévő állomás az IP beállításait közvetlenül az ISP-től kapja.

Sok otthoni és kisebb irodai hálózat egy integrált forgalomirányítót használ az ISP modemjéhez való kapcsolódáshoz. Ebben az esetben a forgalomirányító mind DHCP kiszolgáló, mind ügyfél egyben. Az integrált forgalomirányító, mint ügyfél, az IP beállításait az ISP-től kapja meg, ezután, mint DHCP kiszolgáló viselkedik a belső helyi hálózaton lévő állomások számára.

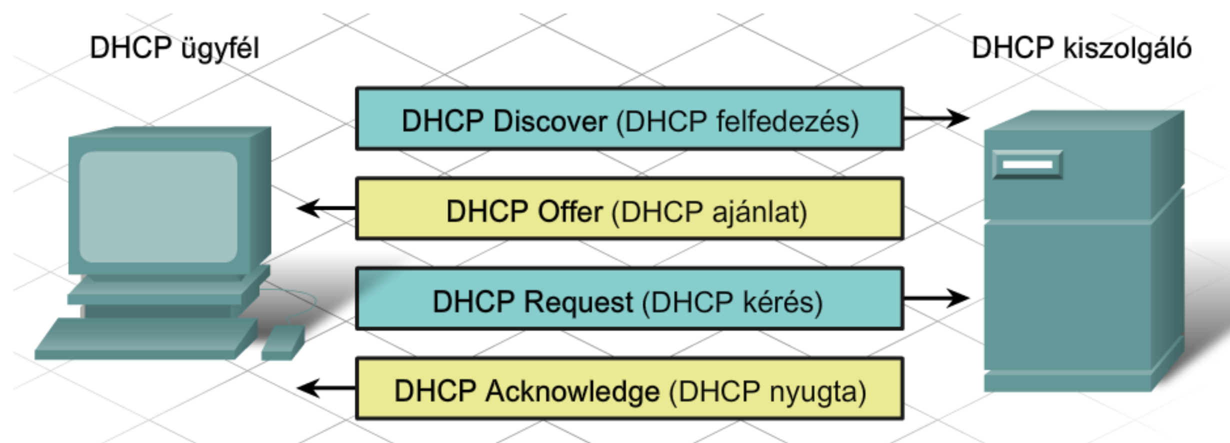
A PC-alapú kiszolgálókon és integrált forgalomirányítókon kívül más típusú hálózati eszközök, mint például dedikált forgalomirányítók is képesek DHCP szolgáltatást nyújtani az ügyfeleknek, bár ez nem olyan gyakori.

5.3.3 A DHCP konfigurálása

Amikor egy állomást először állítunk be DHCP ügyfélként, nem rendelkezik IP címmel, alhálózati maszkkal vagy alapértelmzett átjáróval. Ezt az információt a DHCP kiszolgálótól szerzi be, ami vagy a

helyi hálózaton vagy a szolgáltatónál helyezkedik el. A DHCP kiszolgálót úgy állítják be, hogy legyen az IP címeknek egy tartománya vagy készlete, amiket kioszthat az ügyfeleknek.

Az ügyfél, amelynek IP címre van szüksége egy DHCP felderítés (DHCP Discover) üzenetet küld el 255.255.255.255 cél IP (32 darab egyes), és FF-FF-FF-FF-FF-FF (48 egyesből álló) cél MAC szórási címmel. A hálózat minden állomása fogadja ezt a szórásos DHCP keretet, de csak a DHCP kiszolgáló válaszol rá. A szerver egy felajánlással (DHCP Offer) válaszol, ajánlva egy IP címet az ügyfének. Az állomás ezután elküld egy igénylést (DHCP Request) annak a kiszolgálónak, kérve, hogy használhassa az ajánlott címet. A szerver egy jóváhagyással (DHCP Acknowledgement) válaszol.



A legtöbb otthoni vagy kis irodai hálózaton egy többfunkciós eszköz biztosít DHCP szolgáltatást a helyi hálózat ügyfeleinek. Egy Linksys vezeték nélküli forgalomirányító beállításához nyissuk meg annak grafikus web felületét egy böngésző elindításával és a forgalomirányító alapértelmezett IP címének magadásával: 192.168.1.1. Keressük meg a képernyőt, ami a DHCP beállításokat mutatja.

A 192.168.1.1 IP cím és a 255.255.255.0 alhálózati maszk az alapértelmezettek a forgalomirányító belső interfészén. Ez az alapértelmezett átjáró a helyi hálózat összes állomása számára és egyben a belső DHCP kiszolgáló IP címe is. A legtöbb Linksys vezeték nélküli forgalomirányítón és más otthoni, integrált forgalomirányítón alapértelmezetten engedélyezve van a DHCP kiszolgáló.

A DHCP beállítóképernyőn az alapértelmezett DHCP tartomány hozzáférhető, vagy megadhatunk egy kezdőcímet (ne használjuk a 192.168.1.1-et!) és a kiosztani kívánt címek számát. A bérleti idő is módosítható (az alapértelmezett érték 24 óra). A DHCP beállítási lehetőség a legtöbb ISR-en információt ad a kapcsolódott állomásokról és IP címekről, a hozzájuk tartozó MAC címekről és bérleti időkről.

A DHCP ügyféltáblázat szintén mutatja az ügyfelek neveit és azt, hogy Ethernet LAN-on vagy vezeték nélküli eszközön keresztül kapcsolódtak-e.

5.4 Címek karbantartása

5.4.1 Hálózati határok és címtér

A forgalomirányító egy átjárót biztosít, amin keresztül az egyik hálózaton lévő állomások kommunikálni tudnak más hálózatokon lévő állomásokkal. Egy forgalomirányító minden interfésze más-más hálózatba csatlakozik.

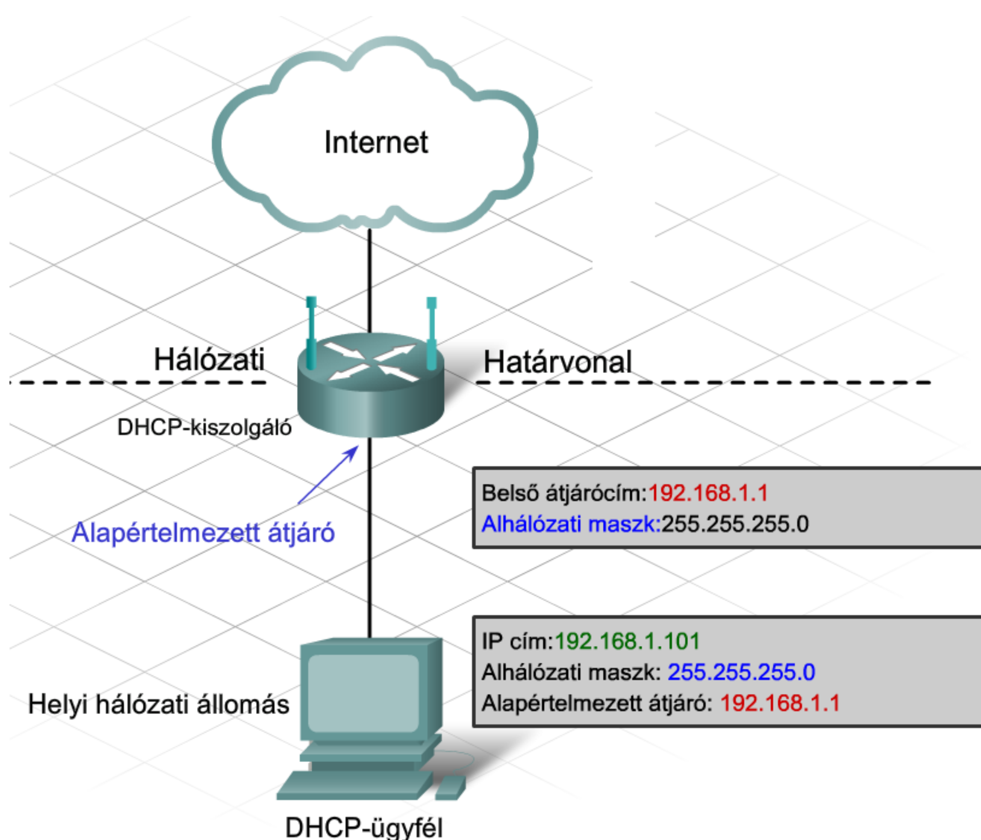
Az interfészhez rendelt IP cím azonosítja, hogy melyik helyi hálózat kapcsolódik hozzá közvetlenül.

Minden helyi hálózaton lévő állomásnak a forgalomirányítót kell átjáróként használnia a többi hálózat felé. Ezért minden állomásnak ismernie kell a forgalomirányító azon csatolójának IP címét, amivel arra a hálózatra csatlakozik, amin az állomás van. Ezt a címet alapértelmezett átjárócímnek hívják. Ezt vagy statikusan adják meg az állomáson, vagy dinamikusan kapja meg DHCP-vel.

Amikor egy integrált forgalomirányítót állítunk be DHCP kiszolgálóként a helyi hálózat számára, automatikusan elküldi a helyes csatolócímet az állomásoknak, mint alapértelmezett átjárócímet. Ily módon az összes hálózati állomás használhatja ezt az IP címet az üzenetek továbbítására az ISP-nél lévő állomások felé, és hozzáférést kap az Internethez. Az integrált forgalomirányítók általában alapértelmezésben DHCP szerverként vannak beállítva.

Ennek a helyi forgalomirányító interfészének az IP címe lesz az alapértelmezett átjáró címe az állomás beállításaiban. Az alapértelmezett átjáró adott, akár statikusan, akár a DHCP által.

Amikor egy integrált forgalomirányítót beállítunk DHCP kiszolgálóként, akkor megadja a saját belső IP címét, mint alapértelmezett átjárót a DHCP ügyfeleknek. Ezen kívül ellátja őket a megfelelő IP címmel és alhálózati maszkkal.



5.4.2 Címek hozzárendelése

Az integrált forgalomirányító DHCP szerverként szerepel az összes hozzá csatlakoztatott helyi állomáson, akár Ethernet kábellel, akár vezeték nélkül csatlakozik. Ezekre a helyi állomásokra úgy hivatkozhatunk, mintha egy belső hálózatban lennének. A legtöbb DHCP kiszolgálót úgy állítják be, hogy magáncímeket szolgáltasson a belső hálózaton lévő állomásoknak ahelyett, hogy az Interneten



irányítható nyilvános címeket adna. Ez biztosítja, hogy alapértelmezésben a belső hálózat nem érhető el közvetlenül az Internetről.

A helyi integrált forgalomirányító csatolójának alapértelmezetten beállított IP címe általában egy magán C osztályú cím. A belső állomásokhoz rendelt címeknek ugyanazon a hálózaton belül kell lenniük, mint az integrált forgalomirányítóé, akár statikusan, akár DHCP-vel kapják. Amikor DHCP kiszolgálóként konfiguráltuk, az integrált forgalomirányító ebből a tartományból ad címeket. Ezen felül megadja az információkat az alhálózati maszkról, valamint a saját interfészének IP címét, mint alapértelmezett átjárót.
Sok szolgáltató szintén DHCP kiszolgálót használ arra, hogy IP címeket osszon ki azon integrált forgalomirányítók Internet felőli oldalán, amiket az előfizetőiknél telepítettek. A hálózatra, ami az integrált forgalomirányító Internet felőli oldalán van, külső hálózatként hivatkozunk.

Amikor egy integrált forgalomirányító csatlakozik a szolgáltatóhoz, úgy viselkedik, mint egy DHCP ügyfél, hogy megkapja a helyes külső hálózati IP címet az Internet interfészéhez. A szolgáltatók általában egy Interneten is irányítható címet adnak, ami lehetővé teszi az integrált forgalomirányítóhoz csatlakozó állomásoknak az Internet elérését.

Az integrált forgalomirányító határként szolgál a belső helyi hálózat és a külső Internet között.

Annak, hogy az állomások kapcsolódjanak a szolgáltatóhoz és az Internethez, több módja van. Az, hogy egy egyedi állomás nyilvános vagy magáncímet kap, attól függ, hogyan kapcsolódik.

Közvetlen kapcsolat

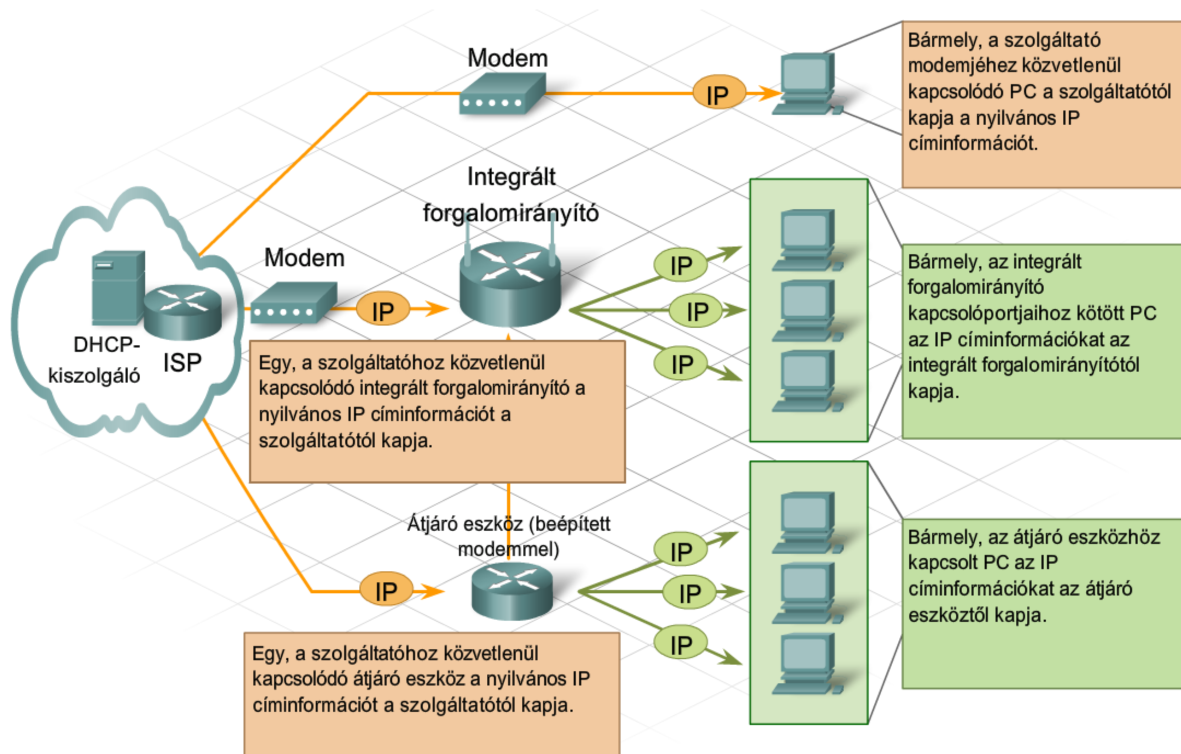
Néhány előfizetőnek csak egyetlen számítógépe van, közvetlen kapcsolattal a szolgáltatótól modemen keresztül. Ebben az esetben az állomás a nyilvános címet a szolgáltató DHCP kiszolgálójától kapja.

Kapcsolódás integrált forgalomirányítón keresztül

Amikor egynél több állomásnak kell hozzáférnie az Internethez, a szolgáltató modemjét közvetlenül egy integrált forgalomirányítóhoz kapcsolhatjuk ahelyett, hogy egyetlen számítógéphez kötnénk. Ez lehetővé teszi egy otthoni vagy kis irodai hálózat kiépítését. Az integrált forgalomirányító a nyilvános címet az ISP-től kapja meg. A belső állomások a magáncímeket az integrált forgalomirányítótól kapják.

Kapcsolódás egy átjáró eszközön keresztül

Az átjáró eszközök egyesítik az integrált forgalomirányítót és a modemet egyetlen egységben, és közvetlenül a szolgáltatóhoz kapcsolódnak. Ahogy az integrált forgalomirányítóknál, az átjáró eszköz a nyilvános címet az ISP-től kapja, a belső PC-k pedig a magáncímeket az átjáró eszköztől.



5.4.3 Hálózati címfordítás

Az integrált forgalomirányító a nyilvános címet a szolgáltatótól kapja, ami lehetővé teszi csomagok küldését és fogadását az Interneten. Ugyanakkor magáncímekkel látja el a helyi hálózat ügyfeleit. Mivel a magáncímek nem engedélyezettek az Interneten, egy olyan folyamatra van szükség, ami átfordítja a magáncímeket egyedi, nyilvános címekké, hogy lehetővé tegye a helyi ügyfelek Internetes kommunikációját.

A folyamatot, ami átalakítja a magáncímeket az Interneten irányítható címekké, hálózati címfordításnak, NAT-nak hívják (Network Address Translation). A NAT segítségével a magán (helyi) forrás IP-címeket nyilvános (globális) címekké alakítjuk. A folyamat megfordul a bejövő csomagoknál. Az integrált forgalomirányító képes sok belső IP cím átfordítására, ugyanarra a nyilvános címre a NAT használatával.

Csak a más hálózatoknak szóló csomagokat kell fordítani. Ezeknek a csomagoknak át kell menniük az átjárón, ahol az integrált forgalomirányító lecseréli a forrásállomás magán IP címét a saját nyilvános IP címére.

Bár minden, a helyi hálózaton lévő állomáshoz rendeltünk egyedi magán IP címet, az állomásoknak osztozniuk kell az egyetlen Interneten irányítható címen, amit az integrált forgalomirányítóhoz rendeltünk.

5.5 A fejezet összefoglalása

IP cím nélkül egy állomás nem tud részt venni az Internet működésében Ez a fejezet összefoglalta az IP címzés fontosságát, annak hierarchikus felépítését és azokat a módszereket, amikkel beszerezhetők a címek egy hálózati eszköz számára.

- Minden logikai IP cím két részből áll: a hálózatazonosítóból és az egyedi állomásazonosítóból azon a hálózaton.
- Egy IP cím 32 bináris számjegy (egyesek és nullák) sorozata, amit négy darab 8 bites csoportba sorolunk, ezeket oktetteknek hívjuk.
- A négy oktett mindegyikét átalakítjuk egy decimális számmá, amire pontozott decimális leírásként hivatkozunk.
- Az IP cím és az alhálózati maszk együttműködik abban, hogy meghatározzák, az IP cím melyik része jelenti a hálózat címét és melyik része az állomásokét.

Az IP címeket több módon is osztályozhatjuk.

- Az IP címeket 5 osztályba soroljuk. Az A, B és C osztály üzleti felhasználású. A D osztály a csoportos címzésre való, az E osztály pedig kísérleti célokra.
- Minden IP címnek megvan a saját alapértelmezett alhálózati maszkja.
- Az IP címeket csoportosíthatjuk úgy is, hogy nyilvánosak vagy magáncélúak. A nyilvános címek egyediek és az Interneten használatosak.
- A magáncímeket az állomások bármely szervezet belső hálózatában használhatják. A magáncímeket át kell alakítani az Interneten irányítható címekké, hogy az állomások kommunikálni tudjanak az Interneten.
- Az állomások az IP címeket egy-az-egyhez (egyedi), egy-a-többhöz (csoportos) vagy egy-mindenkihez (szórásos) kommunikációra használhatják.

Az IP címeket akár statikusan, akár dinamikusan hozzárendelhetjük.

- A statikusan hozzárendelés esetén, az IP címet, az alhálózati maszkot és az alapértelmezett átjárót mind kézzel kell beállítanunk.
- A statikus címeket tipikusan a kiszolgálók igénylik, amiket el kell érni az Internetről.
- A DHCP az előnyben részesített módszer az IP címek hozzárendelésére a nagy hálózatoknál, mivel ez csökkenti a hálózati karbantartó személyzet terhelését.
- Az intergrált forgalomirányító (Integrated Services Router, ISR) ugyanúgy, mint más többfunkciós eszközök, DHCP ügyfélként viselkednek ahhoz, hogy beszerezzék az egyedi IP beállításaikat a szolgáltatótól, ezután pedig DHCP kiszolgálóként, hogy hozzárendeljék az IP címeket a belső állomásokhoz a helyi hálózaton.

A magán IP címeket a szervezeten belülről át kell alakítani egy egyedi nyilvános IP címmé, mielőtt a csomag kimegy az Internetre.

- A forgalomirányítók egy határt képeznek, ami elválasztja a helyi hálózatokat az Internettől.
- Az állomás alapértelmezett átjárója az a forgalomirányító interfész, ami a helyi hálózatra csatlakozik, ezt használják a többi hálózattal való kommunikációra.
- Sok átjáró forgalomirányító átalakítja a magán LAN IP címeket az Interneten irányítható IP címekre egy olyan folyamat segítségével, amit hálózati címfordításnak, NAT-nak hívnak (Network Address Translation).
- Amikor egy vagy több magáncímet átalakítunk egy nyilvános IP címmé, akkor a forgalomirányító nyilvántartja az összes átalakított forrás IP címet és portszámot, hogy a visszatérő forgalmat el tudja juttatni az állomáshoz.

6. Hálózati szolgáltatások

6.1 Ügyfelek, kiszolgálók és kölcsönhatásaik

6.1.1 Az ügyfél-kiszolgáló viszony

Az emberek naponta használják a hálózatokon és az Interneten elérhető szolgáltatásokat másokkal való kommunikációra és rutinfeladatok elvégzésére. Ritkán gondolunk azokra a kiszolgálókra (szerverek), ügyfelekre (kliensek) és hálózati eszközökre, melyek nélkülözhetetlenek számunkra ahhoz, hogy megkapjunk egy elektronikus levelet (e-mail), információt továbbítsunk egy blog-ba vagy akár a legjobb akciós áron vásároljunk egy web-áruházban. Az általánosan használt Internet alkalmazások legnagyobb része több különböző kiszolgáló és ügyfél között zajló összetett kölcsönhatásra (interakciók) támaszkodik.

A kiszolgáló kifejezés egy olyan állomásra (host) vonatkozik, mely a hálózatra csatlakozott más állomások számára információt vagy szolgáltatásokat nyújtó alkalmazást, szoftvert futtat. Egy ilyen alkalmazásra jól ismert példa a webkiszolgáló. Milliónyi kiszolgáló csatlakozik az Internetre olyan szolgáltatásokat nyújtva, mint a webhelyek, elektronikus levelezés, pénzügyi tranzakciók, zeneletöltések stb. Az egyik döntő tényező mely ezeket az összetett kölcsönhatásokat működőképessé teszi az az, hogy mindannyiuk kölcsönösen elfogadott szabványokat és protokollokat használ.

Egy weboldal kérésére és megtekintésére az ember egy olyan eszközt használ, mely web ügyfélprogramot futtat. Az ügyfél olyan számítógépes alkalmazás megnevezése, melyet a kiszolgálón tárolt információhoz való hozzáférésre használunk. Az ügyfélre egy jó példa a webböngésző.

Az ügyfél-kiszolgáló rendszer kulcsjellemzője az, hogy az ügyfél egy kérést (request) küld a kiszolgálónak, a kiszolgáló pedig egy olyan feladat végrehajtásával válaszol, mint például információ megküldése az ügyfél számára. Egy webböngésző és egy webkiszolgáló párosítás talán a legáltalánosabban használt esete az ügyfél-kiszolgáló rendszernek.

Tartománynév kiszolgáló (Domain Name Server, DNS)

- Olyan szolgáltatás, mely biztosítja egy webhely vagy tartománynév IP címét, hogy egy állomás kapcsolódni tudjon hozzá.

Telnet kiszolgáló

- Olyan szolgáltatás, amely megengedi, hogy a kezelők egy távoli helyről bejelentkezzenek egy állomásra és úgy vezéreljék az állomást, mintha helyben jelentkeztek volna be.

Levelezőkiszolgáló

- Egyszerű levéltovábbító protokollt (Simple Mail Transfer Protocol, SMTP), postahivatali protokollt (Post Office Protocol, POP3) vagy Internetes levélhozzáférési protokollt (Internet Message Access Protocol, IMAP) használ.
- Elektronikus levelek küldésére használjuk az ügyféltől a kiszolgálóig az Interneten keresztül.
- A címzettek megadása felhasznalo@xyz forma használatával történik.

A dinamikus állomáskonfigurációs protokol (Dynamic Host Configuration Protocol, DHCP) kiszolgáló

- Olyan szolgáltatás, mely az ügyfelek számára IP címeket, alhálózati maszkot, alapértelmezett átjárót és más információt jelöl ki.

Webkiszolgáló

- Hiperszöveg átviteli protokoll (HyperText Transfer Protocol, HTTP)
- A web ügyfél és webkiszolgáló közötti információátvitelre használjuk.
- A legtöbb weboldalhoz HTTP használatával férünk hozzá.

Fájlátviteli protokoll (File Transfer Protocol, FTP

- Olyan szolgáltatás mely megengedi állományok letöltését illetve feltöltését az ügyfél és a kiszolgáló között.

6.1.2 A protokoll szerepe az ügyfél-kiszolgálói kommunikációban

Egy web kiszolgáló és egy web ügyfél az információcsere folyamatában speciális protokollokat és szabványokat használ annak biztosítására, hogy az üzenetek megérkezzenek és azokat meg is értsék. Ezek a protokollok felölelik az alkalmazási, szállítási, hálózati és hálózatelérési protokollokat.

Alkalmazási protokoll

A hiperszöveg átviteli protokoll (Hypertext Transfer Protocol, HTTP) a web kiszolgáló és web ügyfél kölcsönhatásának módját szabályozza. A HTTP meghatározza az ügyfél és a kiszolgáló közötti kérések és válaszok formáját. A HTTP más protokollokra bízza azt, hogy az üzenetek hogyan kerüljenek szállításra az ügyfél és a kiszolgáló között.

Szállítási protokoll

Az átvitel-vezérlési protokoll (Transmission Control Protocol, TCP) az, amely kezeli a web kiszolgálók és a web ügyfelek közötti egyedi párbeszédet. A TCP a HTTP üzeneteket a célállomás számára eküldendő szegmensekké alakítja. Ezenkívül biztosítja az adatfolyamvezérlést és az állomások között kicserélt csomagok nyugtázását.

Hálózati protokoll

A legáltalánosabb hálózati protokoll az Internet protokoll (Internet Protocol, IP). Az IP felelős a kialakított szegmensek TCP-től való átvételéért, azokhoz logikai címzés hozzárendeléséért és csomagokba történő beágyazásukért és a célállomáshoz irányításért.

HTTP: megszabja a weboldalra vonatkozó kérés (ügyfél részéről) és a válasz (kiszolgáló részéről) formáját

TCP: meghatározza az áramlásvezérlést és a csomagcserék nyugtázását

IP: azonosítja a forrást és a célt, amint a csomagok küldésre kerülnek a hálózaton

Hálózatelérési protokollok

Helyi hálózatoknál az Ethernet a legáltalánosabban használt protokoll. A hálózatelérési protokollok két elsődleges feldatot látnak el, az adatkapcsolat kezelését és a fizikai hálózati átviteleket.

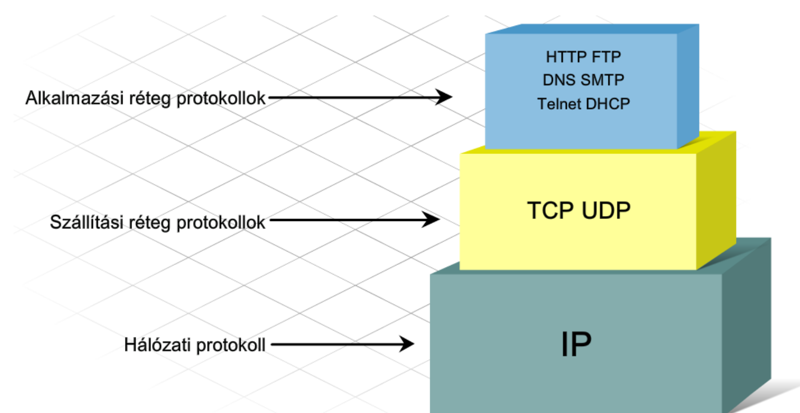
Az adatkapcsolat kezelési protokollok átveszik az IP-től a csomagokat és a helyi hálózatnak megfelelő formátumú keretbe ágyazzák őket. Ezek a protokollok rendelik a fizikai címet a keretekhez és készítik elő őket a hálózaton való továbbításra.

A fizikai közeg szabványai és protokolljai azt szabályozzák, hogy milyen módon kerülnek a bitek ábrázolásra a közegben, hogyan kerülnek a jelek a közegben továbbításra és hogyan értelmezzék őket a fogadó állomások. Hálózati illesztőkártyák valósítják meg a használt közeg számára alkalmas protokollokat.

6.1.3 TCP és UDP szállítási protokollok

A hálózaton rendelkezésre álló minden szolgáltatás saját alkalmazási protokollal rendelkezik, melyek kiszolgálói és ügyfél szoftverekben kerülnek megvalósításra. Az alkalmazási protokollok és minden általánosan használt Internet szolgáltatás az Internet protokollt (IP) használja címzésre és az üzenetek forrás és a cél közötti irányítására.

Az IP csak a struktúrával, a címzéssel és csomagok irányításával törődik. Az IP nem határozza meg, hogy hogyan történjen a csomagok elszállítása vagy kézbesítése. A szállítási protokoll határozza meg, hogy hogyan történjen az üzenetek átvitele az állomások között. A két legáltalánosabb szállítási protokoll az átvitel-vezérlési protokoll (Transfer Control Protocol, TCP) és a felhasználói adategység protokoll (User Datagram Protocol, UDP). Az IP ezeket a szállítási protokollokat használja az állomások közötti kommunikáció biztosítására és az adatok átvitelére.



Ha egy alkalmazásnak nyugtára van szüksége arról, hogy az üzenet megérkezett, akkor TCP-t használ. Ez hasonló ahhoz, mikor a postán keresztül egy tértivevényes levelet küldünk, mikoris a címzettnek aláírásával kell nyugtáznia, hogy megkapta a levelet.

A TCP, szegmensnek nevezett kis részekre darabolja szét az üzenetet. A szegmensek sorszámot kapnak, majd az IP folyamathoz kerülnek a csomag összeállítása céljából. A TCP figyelemmel kíséri azokat a szegmens sorszámokat, melyeket az adott alkalmazástól már elküldött a meghatározott állomásnak. Ha a küldő nem kap nyugtát egy bizonyos időn belül, azt feltételezi, hogy a szegmens elveszett, ezért azt újraküldi. Az elveszett üzenetnek csak egy kis része kerül újraküldésre, nem maga a teljes üzenet.

A címzett állomás esetén a TCP felelős az üzenetszegmensek összeillesztéséért és az alkalmazáshoz való továbbításáért.

Az FTP és a HTTP egy-egy példa azokra az alkalmazásokra, melyek a TCP-t használják azért, hogy gondoskodjanak az adatok kézbesítéséről.

Néhány esetben nincs szükség a TCP nyugtázásos protokollra és valójában le is lassítja az információ továbbítását. Ilyen esetekben az UDP lehet a megfelelőbb szállítási protokoll.

Az UDP egy 'legjobb szándék' szerint kézbesítő (best effort delivery) rendszer, mely nem igényel a vételről nyugtázást. Ez hasonló ahhoz, mikor a postán egy hagyományos levelet küldünk el. Nincs garancia arra, hogy a levelet megkapja a címzett, de jó esély van rá.

Az UDP olyan alkalmazásoknál részesül előnyben, mint a video- és audiófolyam, IP alapú VoIP hangtovábbítás. A nyugtázás lelassítaná a kézbesítést és az újraküldés sem kívánatos.

Az UDP-t használó alkalmazásra egy példa az Internet rádió. Ha az üzenet egy része a hálózaton megtett út során elveszik, az nem kerül újratovábbításra. Ha néhány csomag hiányzik, a hallgató esetleg egy kis fennakadást hallhat a hangnál. Ha a TCP-t használnánk és az elvesztett csomagok újraküldésre kerülnének, az adattovábbítás szünetelne annak érdekében, hogy megkapjuk őket és ez a hangkimaradás még észrevehetőbb volna.

6.1.4 TCP/IP portszámok

Ha egy üzenet kézbesítésre kerül akár TCP akár UDP segítségével, a protokollok és a kért szolgáltatások azonosítása egy portszámmal történik. A port egy számszerű azonosító minden egyes szegmensben, amely a párbeszédek és a kért célszolgáltatások nyomon követésére szolgál. Minden üzenet, melyet egy állomás elküld, tartalmaz mind egy forrás-, mind egy célportot.

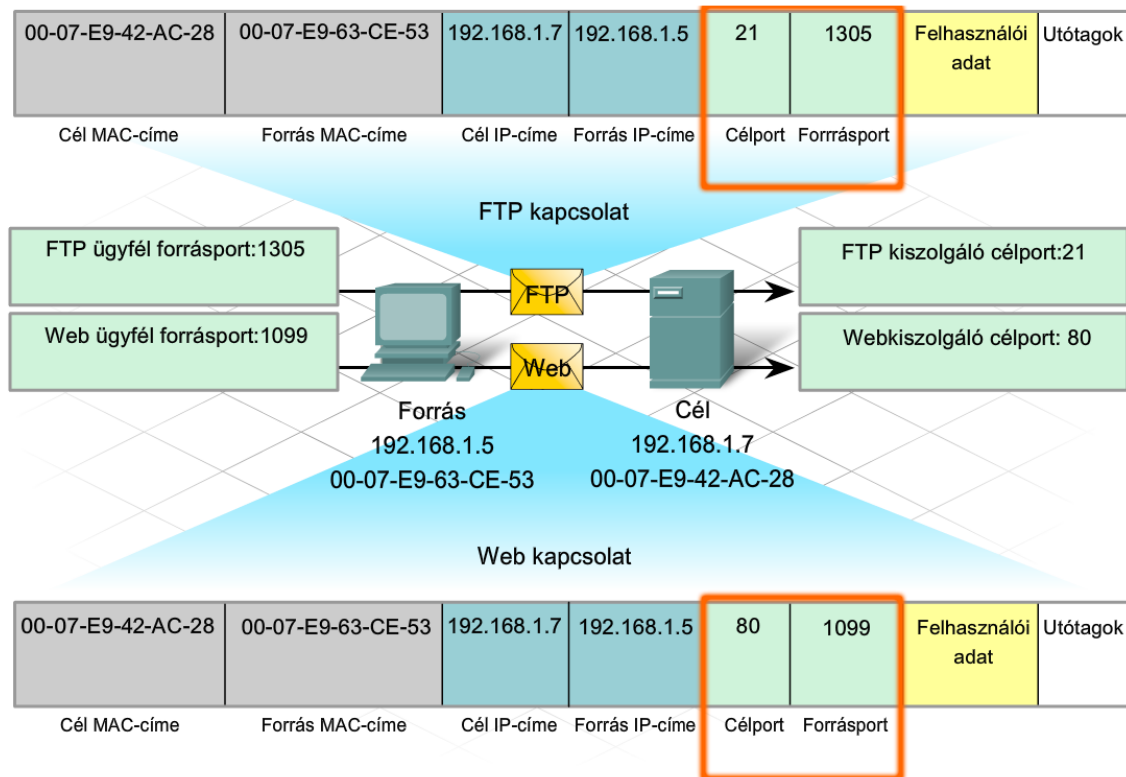
Célport

Az ügyfél, hogy közölje a cél kiszolgálóval, hogy milyen szolgáltatást kér, elhelyez egy célport számot a szegmensben. Például a 80-as port a HTTP-re vagyis a web szolgáltatásra utal. Amikor az ügyfél célportként a 80-as portot adja meg, a kiszolgáló, amelyik az üzenetet megkapja tudja, hogy web szolgáltatást kértek. Egy kiszolgáló párhuzamosan több szolgáltatást is kínálhat Például egy kiszolgáló web szolgáltatást nyújthat a 80-as porton, ugyanakkor FTP csatlakozás felépítését is kínálhatja a 21-es porton.

Forrásport

A forrásport számot véletlenszerűen generálja a küldő eszköz a két eszköz közötti párbeszéd azonosítására. Ez párhuzamosan több párbeszédet tesz lehetővé. Másszóval ugyanabban az időben több eszköz kérhet HTTP szolgáltatást egy web kiszolgálótól. Az elkülönített párbeszédek nyomon követése a forrásportokon alapszik.

A forrás és célportok a szegmensben kerülnek elhelyezésre. A szegmensek ezt követően egy IP csomagba kerülnek beágyazásra. Az IP csomag tartalmazza a forrás és a cél IP-címét. A forrás és cél IP-címek, valamint a forrás és cél portszámok kombinációja által meghatározott kommunikációs csatorna, socket (csatlakozó) néven ismert. A socket használatos a kiszolgáló és az ügyfél által kért szolgáltatás azonosítására. Naponta állomások ezrei kommunikálnak ezernyi különböző kiszolgálóval. Ezeket a kommunikációkat a socket azonosítja.



6.2 Alkalmazási protokollok és szolgáltatások

6.2.1 Tartománynév szolgáltatás (Domain Name Service, DNS)

Számos különböző helyszínen telepített ezernyi kiszolgáló biztosítja azokat a szolgáltatásokat, melyeket naponta használunk az Interneten. A kiszolgálók mindegyikéhez egy egyedi IP-cím kerül kijelölésre, mely azonosítja őket azon a helyi hálózaton, melyhez kapcsolódnak.

Lehetetlen lenne megjegyezni az Interneten szolgáltatást nyújtó minden egyes kiszolgáló IP-címét. Ehelyett van egy könnyebb módja a kiszolgálók kijelölésének, mégpedig egy IP-cím és egy név társítása.

A tartománynév rendszer (Domain Name System) DNS egy módszert biztosít az állomások számára ahhoz, hogy ezt a nevet használják egy meghatározott kiszolgáló IP-címének kéréséhez. A DNS nevek bejegyzett nevek és az Interneten bizonyos legfelsőbb szintű csoportokba, vagy tartományokba szervezik őket. Néhány az Interneten használt legáltalánosabb legfelsőbb szintű tartomáynnév a .com, .edu és a .net.

A DNS kiszolgáló egy olyan táblát tartalmaz, mely a tartomány állomásneveit a megfelelő IP címekhez társítja. Amikor az ügyfél rendelkezik a kiszolgáló nevével, mint például egy web kiszolgálóéval, és

meg kell találnia az IP-címet, akkor egy kérést küld a DNS kiszolgálónak az 53-as porton. Az ügyfél az állomás IP konfigurációjának DNS beállításainál megadott DNS kiszolgáló IP-címét használja.

Amikor a DNS kiszolgáló megkapja a kérést, megvizsgálja a táblát hogy meghatározza az adott web kiszolgálóhoz társított IP címet. Ha a helyi DNS kiszolgáló nem rendelkezik az igényelt névre vonatkozó bejegyzéssel, akkor lekérdezi a tartományban található másik DNS kiszolgálót. Amikor a DNS kiszolgáló megtudja az IP-címet, ezt az információt megküldi az ügyfélnek. Ha a DNS kiszolgáló nem képes meghatározni az IP számot, a kérés túllépi az időkorlátot, így az ügyfél képtelen lesz kommunikálni az adott web kiszolgálóval.

Az IP-címek megszerzésében az ügyfélprogram a DNS protokollal olyan módon működik együtt, hogy ez a felhasználó számára láthatatlan.

6.2.2 Web ügyfelek és kiszolgálók

Amikor egy web ügyfél megkapja egy web kiszolgáló IP címét, az ügyfél böngészőprogramja az IP címet és a 80-as portot használja a webszolgáltatás kéréséhez. Ezt a kérést a hiperszöveg átviteli protokoll (HyperText Transfer Protocol, HTTP) felhasználásával küldi meg a kiszolgálónak.

Amikor a kiszolgáló megkap egy 80-as portszámú kérést, a kiszolgáló válaszol az ügyfél kérésére és megküldi a weboldalt az ügyfélnek. A weboldal információtartalma egy speciális 'leíró' nyelv felhasználásával kerül kódolásra. A legáltalánosabban használt nyelv a HTML (HyperText Mark-up Language, hiperszöveg leíró nyelv), de mások is egyre nagyobb népszerűségnek örvendenek, mint például az XML és XHTML.

A HTTP protokoll egy nem megbízható protokoll; az információt más felhasználók is könnyedén elfoghatják amint azt a hálózaton küldjük. Az adatok védelmének biztosítása érdekében a HTTP biztonságos szállítási protokollal is használható. A biztonságos HTTP kérés megküldése a 443-as portra történik. Ezeknél a kéréseknél a webhely címénél a böngészőben a http: helyett a https: -t kell használni.

A piacon számos különböző web szolgáltatás és web ügyfél áll rendelkezésre. A HTTP protokoll és a HTML teszi lehetővé azt, hogy a legkülönbözőbb gyártóktól származó kiszolgálók és ügyfelek akadálymentesen együttműködjenek.

6.2.3 FTP ügyfelek és kiszolgálók

A web szolgáltatásokon kívül az Interneten használt más általános szolgáltatások egyike az, amelyik lehetővé teszi a felhasználók számára az állományok átvitelét.

A fájlátviteli protokoll (File Transfer Protocol, FTP) egy egyszerű módszert biztosít az állományok egyik számítógépről a másikra történő átvitelére. Egy FTP ügyfélprogramot futtató állomás hozzáférhet egy FTP kiszolgálóhoz különféle állománykezelési műveletek végrehajtása - köztük az állomány feltöltése és letöltése - érdekében.

Az FTP kiszolgáló az eszközök közötti állománycserét teszi lehetővé az ügyfél számára. Azt is lehetővé teszi, hogy az ügyfél olyan állománykezelő parancsok küldésével, mint például a törlés (delete) vagy az átnevezés (rename), távolról kezelje az állományokat. Ennek megvalósítására az FTP szolgáltatás két különböző portot használ a kiszolgáló és az ügyfél közötti kommunikációra.

Egy FTP munkamenet megkezdése iránti kérés a 21-es célportot használó kiszolgáló számára kerül megküldésre. Amennyiben a munkamenet megnyílt, a kiszolgáló az állományok átviteléhez a 20-as portra vált át.

Az FTP ügyfélprogram beépítésre kerül a számítógép operációs rendszerébe és a legtöbb web böngészőbe is. Az önálló FTP ügyfélprogramok számos további lehetőséget és egy könnyen használható grafikus felületet (GUI) biztosítanak.

6.2.4 E-mail ügyfelek és kiszolgálók

Az e-mail egyike az Internet legnépszerűbb ügyfél-kiszolgáló alapú szolgáltatásainak. Az e-mail kiszolgálók olyan kiszolgáló programot futtatnak, mely lehetővé teszi azt, hogy a hálózaton keresztül kölcsönhatásba lépjenek az ügyfelekkel és más e-mail kiszolgálókkal.

Mindegyik levelezési kiszolgáló fogadja és tárolja azoknak a felhasználóknak a leveleit, kik beállított postafiókkal rendelkeznek a levelezési kiszolgálón. Mindegyik postafiókkal rendelkező felhasználónak egy e-mail ügyfélprogramot kell használnia ahhoz, hogy hozzáférjen a levelezési kiszolgálóhoz és el tudja olvasni ezeket az üzeneteket.

A levelezési kiszolgálókat ezenkívül arra is szokták használni, hogy elküldjék a helyi postafiók vagy más levelezési kiszolgálón található postafiók címére címzett levelet.

A postafiókok azonosítása az alábbi formában történik:

felhasznalo@tarsasag.tartomany

Az elektronikus levelek feldolgozásakor különféle alkalmazási protokollokat használunk, mint például az SMTP, POP3, IMAP4.

Egyszerű levéltovábbító protokoll (Simple Mail Transfer Protocol, SMTP)

Az SMTP-t az e-mail ügyfél arra használja, hogy elküldje az üzenetet a helyi e-mail kiszolgálójának. A helyi kiszolgáló ezután eldönti, hogy vajon az üzenetet egy helyi postafióknak szánták, vagy egy másik kiszolgáló postafiókjának címezték.

Ha a kiszolgálónak az üzenetet egy másik kiszolgálóhoz kell elküldenie, a két szerver egymás között szintén az SMTP-t használja. A SMTP kérés elküldése a 25-ös portra történik.

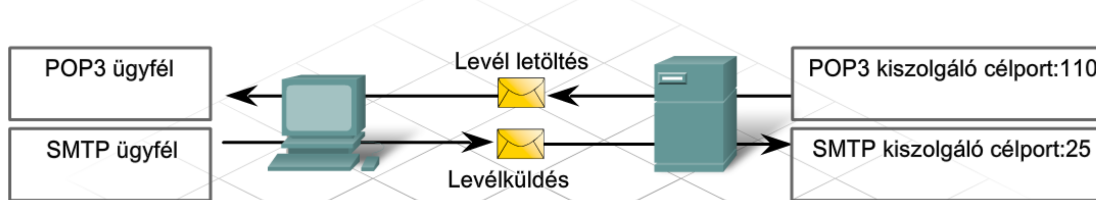
Postahivatali protokoll (Post Office Protocol, POP3)

Az a kiszolgáló mely támogatja a POP ügyfeleket, fogadja és tárolja a felhasználói számára címzett üzeneteket. Amikor az ügyfél az e-mail kiszolgálóhoz kapcsolódik, az üzenetek letöltésre kerülnek az ügyfélhez. Alapesetben az üzenetek nem maradnak a kiszolgálón azt követően, hogy az ügyfél már hozzájuk fért. Az ügyfél a POP3 kiszolgálóval a 110-es porton lép kapcsolatba.

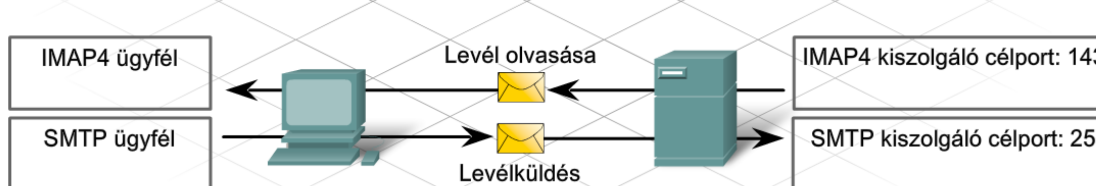
Internetes levélhozzáférési protokoll (Internet Message Access Protocol, IMAP)

Az a kiszolgáló, mely az IMAP ügyfeleket támogatja, szintén fogadja és tárolja a felhasználóinak címzett üzeneteket. Azonban az üzeneteket megtartja a kiszolgálón található postafiókban, hacsak azokat maga a felhasználó nem törli. Az IMAP legfrissebb változata az IMAP4, mely az ügyfél kéréseit a 143-as porton figyeli.

A különböző hálózati operációs rendszer platformokra számos különböző e-mail kiszolgáló létezik.



POP3: Az ügyfél használja a kiszolgálóhoz történő kapcsolódásra és a levelek letöltésére. A levelek törlésre kerülnek a kiszolgálóról.
SMTP: Az ügyfél használja a levél továbbítására a kiszolgálóhoz. A szerver fogadja és a megfelelő sorban eltárolja a levelet.



IMAP4: Az ügyfél használja a kiszolgálóhoz történő kapcsolódásra és a levelekhez történő hozzáférésre. A levelek kezelése a kiszolgálón történik.
SMTP: Az ügyfél használja a levél továbbítására a kiszolgálóhoz. A szerver fogadja és a megfelelő sorban eltárolja a levelet.

Az e-mail kiszolgálóhoz egy e-mail ügyfél csatlakozik az üzenetek megtekintése és letöltése céljából. A legtöbb e-mail ügyfél akár a POP3, akár az IMAP4 használatára beállítható attól az e-mail kiszolgálótól függően, ahol a postafiók található. Az e-mail ügyfeleknek képeseknek kell lenniük arra is, hogy az SMTP használatával elektronikus levelet küldjenek a kiszolgálónak.

A bejövő irányú és a kimenő irányú levelezéshez eltérő e-mail kiszolgálók is beállíthatók.

Amikor egy e-mail ügyfelet állítunk be, tipikusan az alábbiakat kell megadnunk:

- POP3 vagy IMAP4 kiszolgáló neve
- SMTP kiszolgáló neve
- Felhasználó neve
- Felhasználó jelszava
- SPAM vagy vírusszűrők

Az ábra egy POP3 és SMTP e-mail fiók alapbeállításait mutatja Microsoft Outlook használata esetén.

6.2.5 IM ügyfelek és kiszolgálók

Az azonnali üzenetküldés (Instant Messaging, IM) egyike a napjainkban használt legnépszerűbb kommunikációs eszközöknek. Az IM szoftver mindegyik számítógépen helyileg fut és lehetővé teszi a felhasználóknak, hogy az Interneten keresztül valós időben kommuniáljanak vagy csevegjenek. Különféle társaságok számos különböző IM alkalmazása áll rendelkezésre. Minden egyes azonnali üzenetküldő szolgáltatás eltérő protokollokat és célportokat használhat, így a kommunikációhoz a két állomáson telepített IM szoftvernek egymással kompatibilisnek kell lennie.

AZ IM alkalmazások a működéshez minimális beállítást igényelnek. Amennyiben az ügyfél már letöltésre került, mindössze a felhasználói név és a jelszó megadása szükséges. Ez teszi lehetővé az IM ügyfél hitelesítését az IM hálózaton. Ha az ügyfél már bejelentkezett a kiszolgálón, akkor valós

időben küldhet üzeneteket más ügyfeleknek. A szöveges üzeneteken kívül az IM támogatja a mozgókép (video), zene és beszédhang állományok átvitelét is. Az IM ügyfél rendelkezhet telefonálási tulajdonságokkal is, mely lehetővé teszi hogy a felhasználó telefonhívásokat kezdeményezzen az Interneten keresztül. További beállítások is elvégezhetők, hogy a "Haverok listája" illetve személyes kép és érzés alapján az IM ügyfelet testre tudjuk szabni.

Az IM ügyfélprogram minden típusú állomásra letölthető és ott használható többek között: számítógépeken, PDA-kon és mobiltelefonokon.

6.2.6 Hangtovábbítási (voice) ügyfelek és kiszolgálók

Az Interneten keresztül történő telefonálás egyre inkább népszerűvé válik. Egy Internet telefon ügyfél egyenrangú kommunikációs technológiát (peer-to-peer) használ hasonlóan ahhoz, mint amilyet az azonnali üzenetküldés is használ. Az IP telefon az IP-vel történő hangtovábbítási (Voice over IP, VoIP) technológiát használja ki, mely IP csomagokat használ a digitalizált hangnak, mint adatnak a továbbítására.

Az Internet telefon használatának megkezdéséhez töltsd le a kliensszoftvert azon társaságok egyikétől melyek ezt a szolgáltatást nyújtják. Az Internet telefon díjak nagy mértékben változhatnak a különböző régiók és szolgáltatók függvényében.

Ha a szoftver már telepítve lett, a felhasználó kiválaszt egy egyedi nevet. Ez azért van, hogy fogadni lehessen más felhasználótól érkező hívást. Szükség van beépített, vagy különálló hangszóróra és mikrofonra. Telefonként gyakran egy a számítógéphez csatlakoztatott, mikrofonnal ellátott fejhallgató (headset) szolgál.

Az Internet ugyanezen szolgáltatását igénybe vevő más felhasználók felhívása a felhasználó nevének a kiválasztásával történik a listából. Egy hagyományos telefon (vezetékes vagy mobil) felhívásához egy átjáróra (gateway) van szükségönk, hogy hozzáférjünk a nyilvános kapcsolású telefonhálózathoz (Public Switched Telephone Network, PSTN).

Az Internet telefon alkalmazás által használt protokollok és célportok a szoftvertől függően változhatnak.

6.2.7 Portszámok

A DNS, Web, E-mail, FTP, IM és VoIP csak néhány, az Internet ügyfél-kiszolgáló rendszerei által nyújtott számos szolgáltatás közül. Ezeket a szolgáltatásokat egyetlen kiszolgáló vagy több kiszolgáló is biztosíthatja.

Egy kiszolgálóra minden esetben szükség van annak megismeréséhez, hogy melyik szolgáltatást kéri az ügyfél. Az ügyfél kérései azonosíthatók, mivel a kérés egy meghatározott célportra irányul. Az ügyfelek előzetesen úgy kerülnek beállításra, hogy minden szolgáltatáshoz egy olyan célportot használjanak, mely már bejegyzésre került az Interneten.

A portok három kategóriára vannak osztva és a számtartományuk 1-től 65535-ig terjed. A portok kijelölését és kezelését egy 'Kijelölt Nevek és Számok Internet Testülete' (Internet Corporation for Assigned Names and Numbers, ICANN) néven ismert szervezet végzi.

Közismert portok

Azokat a célportokat melyek általános hálózati alkalmazásokhoz társulnak közismert portként azonosítjuk. Ezeknek a portoknak a számtartománya 1-től 1023-ig terjed.

Bejegyzett portok

Az 1024 és 49151 közötti portok, melyek mind forrás, mind célportként használhatók. Szervezetek használhatják ezeket olyan sajátos alkalmazások bejegyzésére, mint az IM alkalmazások.

Egyéni portok

A 49152 és 65535 közötti portok, melyeket gyakran forrásportként használnak. Ezeket a portokat bármely alkalmazás használhatja.

A táblázat néhány gyakoribb közismert portot mutat.

Célportszám	Rövidítés	Definíció
20	FTP Adat	Fájlátviteli protokoll (File Transfer Protocol) (adatátvitelhez)
21	FTP Vezérlés	Fájlátviteli protokoll (File Transfer Protocol) (kapcsolat felépítéshez)
23	TELNET	Távgépíró hálózat (TELetype NETwork)
25	SMTP	Egyszerű levéltovábbító protokoll (Simple Mail Transfer Protocol)
53	DNS	Tartománynév szolgáltatás (Domain Name Service)
67	DHCP v4 ügyfél	Dinamikus állomáskonfigurálási protokoll (Dynamic Host Configuration Protocol) (ügyfél)
68	DHCP v4 kiszolgáló	Dinamikus állomáskonfigurálási protokoll (Dynamic Host Configuration Protocol) (kiszolgáló)
69	TFTP	Triviális fájlátviteli protokoll (Trivial File Transfer Protocol)
80	HTTP	Hiperszöveg átviteli protokoll (Hypertext Transfer Protocol)
110	POP3	Postahivatal protokoll (Post Office Protocol) (3-as verzió)
137	NBNS	Microsoft NetBIOS névszolgáltatás (NetBios Name Service)
143	IMAP4	Internetes levél hozzáférési protokoll (Internet Message Access Protocol) (4-es verzió)
161	SNMP	Egyszerű hálózatfelügyeleti protokoll (Simple Network Management Protocol)
443	HTTPS	Biztonságos hiperszöveg átviteli protokol (Hypertext Transfer Protocol Secure)

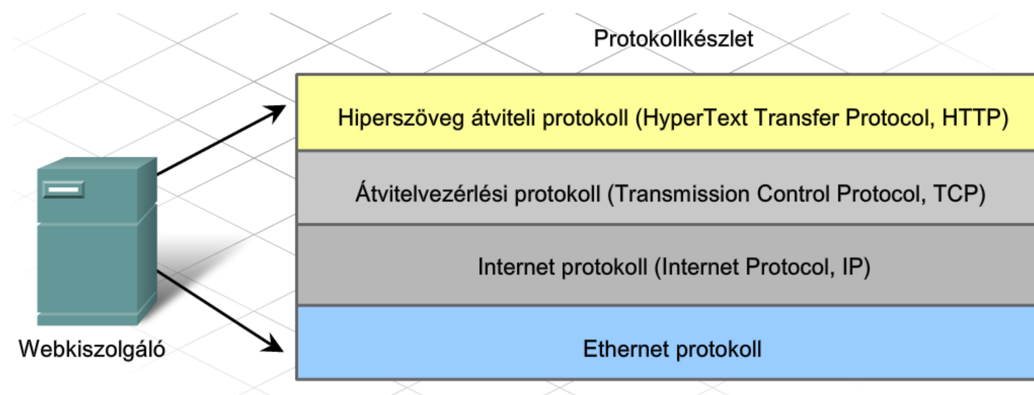
6.3 A rétegmodell és a protokollok

6.3.1 A protokollok kölcsönhatása

Az állomások közötti sikeres kommunikáció számos protokoll egymás közti kölcsönhatását igényli. Ezek a protokollok olyan szoftverben és harverben kerülnek megvalósításra, amely minden állomáson és hálózati eszközön telepítésre kerül.

A protokollok közötti kölcsönhatást protokollkészletként ábrázolhatjuk. Ez a protokollokat az egymás alá- és fölé rendelt rétegek hierarchiájaként mutatja úgy, hogy minden egyes magasabb szintű protokoll az alsóbb rétegekben látható protokollok szolgáltatásaitól függ.

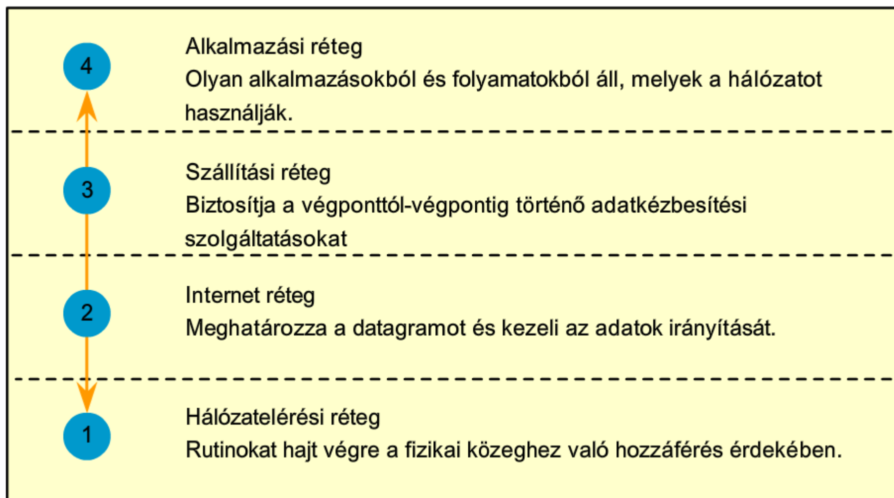
Az ábra egy protokollkészletet mutat olyan elsődleges protokollokkal, melyek egy web kiszolgáló futtatásához szükségesek az Etherneten. A készlet alsóbb rétegei az adatok hálózaton belüli mozgatását és a felsőbb rétegek számára történő szolgáltatások nyújtását végzik. A felsőbb rétegek inkább a küldendő üzenet tartalmára és a felhasználói interfészre összpontosítanak



A különféle protokollok közötti kölcsönhatások szemléltetésének általánosan használt eszköze a rétegmodell. A rétegmodell az egyes rétegekben található protokollok működését és az alatta, illetve a fölötte levő rétegekkel történő kölcsönhatását ábrázolja.
A rétegmodellnek számos előnye van:

- Segít a protokolltervezésnél, mert egy adott rétegben működő protokoll esetén egyértelműen specifikált, hogy mit kell tennie és, hogy milyenek az alsóbb illetve a felsőbb rétegek felé használható interfészei.
- Elősegíti a versenyt, mivel a különböző gyártóktól származó termékek képesek együtt működni.
- Véd attól, hogy az egyik réteg technológiájának vagy adottságainak változásai hatással legyenek az alatta vagy a felette levő másik rétegre.
- Általános nyelvet biztosít a hálózat működésének és képességeinek leírásához.

A hálózatközi kommunikáció első rétegmodellje az 1970-es évek elején került kidolgozásra, melyet Internet modellnek nevezünk. Meghatározta a működés azon négy kategóriáját mely nélkülözhetetlen a sikeres kommunikációhoz. A TCP/IP protokollok szerkezete ennek a modellnek a struktűráját követi. Ezért általában az Internet modellt úgy nevezzük hogy TCP/IP modell.



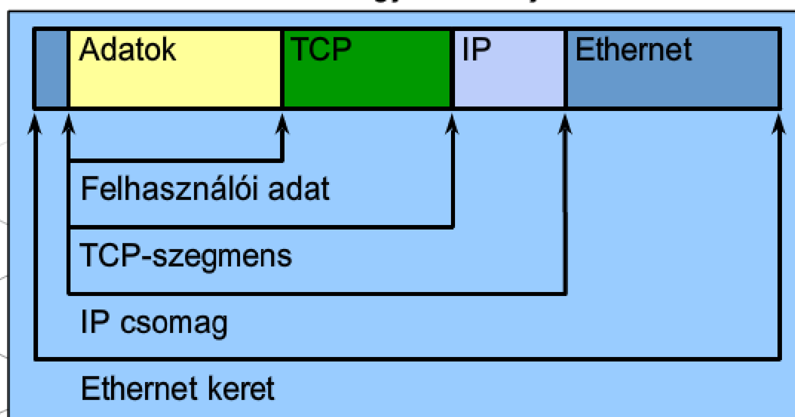
6.3.2 Protokollműködés egy üzenet küldése és fogadása során

A hálózaton történő üzenetküldésnél az állomás protokollkészlete felülről lefelé aktiválódik. Egy web kiszolgálónál az ügyfél-gépen futó böngészőprogram a 80-as célporton egy web lapot kér a kiszolgálótól. Ezzel indul a web oldal ügyfélhez való küldésének folyamata.

Amint a web oldal leküldésre kerül a web kiszolgáló protokollkészletéhez, az alkalmazási adat TCP szegmensekre darabolódik. Minden TCP szegmenshez egy fejrész adódik mely tartalmazza a forrás és a célportot.

A TCP szegmens beágyazza a HTTP protokollt és a web oldal HTML felhasználói adatait, majd leküldi azt az alatta levő szomszédos protokollrétegnek, amely az IP. Itt a TCP szegmens beágyazásra kerül egy IP csomagba mely IP fejrésszel egészül ki. Az IP fejrész a forrás és cél IP címeket tartalmazza.

Ezt követően az IP csomag az Ethernet protokollhoz kerül megküldésre, ahol beágyazódik egy keret fejrész és utótag közé. Minden egyes Ethernet keret fejrész egy forrás és cél MAC címet tartalmaz. Az utótag hibaellenőrzési információt tartalmaz. Végül a biteket a kiszolgáló hálózati illesztőkártyája (NIC) kódolja át az Ethernet közegnek (réz vagy optikai kábel) megfelelő jelekké.



Amikor a hálózatról üzenetet kapunk, akkor az állomáson található protokollkészlet alulról felfelé működik. Az előzőekben rétegenként láttuk a beágyazás folyamatát, amikor a web kiszolgáló

weboldalt küldött az ügyfélnek. A weboldal fogadásának folyamatával megkezdődik az üzenet ügyfél által történő kicsomagolása.

Amikor az ügyfél NIC fogadja a biteket, dekódolja és a cél MAC cím alapján megállapítja, hogy az üzenetet neki címezték.

A keret a web ügyfél protokollkészletéhez kerül, amely eltávolítja az Ethernet fejrészt (forrás és cél MAC cím) és az utótagot (kicsomagolás). A megmaradt IP csomag és tartalma az IP réteghez kerül).

Az IP réteg eltávolítja az IP fejrészt (forrás és cél IP cím), majd a csomag tartalmát a TCP réteghez továbbítja.

A TCP réteg eltávolítja a TCP fejrészt (forrás- és célportok) és a weboldal felhasználói adattartalmát a felette működő és HTTP-t használó böngésző alkalmazás kapja meg. Ahogy a TCP szegmensek folyamtosan érkeznek, tartalmukból összeáll az eredeti weboldal.

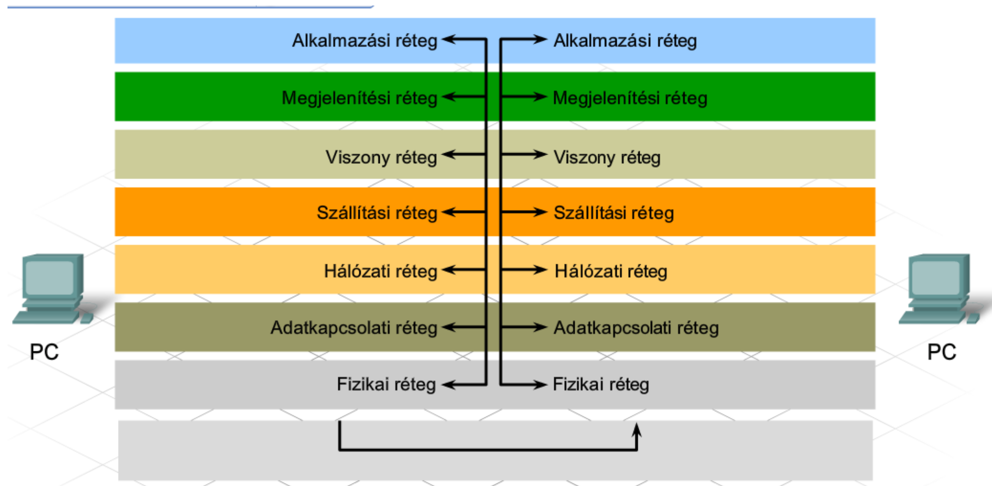
6.3.3 A nyílt rendszerek összekapcsolódása modell

A nyílt rendszerek összekapcsolása modellt (Open Systems Interconnect Model) a Nemzetközi Szabványügyi Szervezet (International Organization for Standardization, ISO) fejlesztette ki 1984-ben. A TCP/IP modelltől eltérően ez semmilyen különleges protokollok kölcsönhatását nem határozza meg. Egy követendő szerkezetnek készült a hálózati kommunikáció számára történő protokolltervezéshez a fejlesztők számára. Habár nagyon kevés protokollverem valósítja meg pontosan az OSI modell hét rétegét, jelenleg ezt tekintik a számítógépek közötti kommunikáció elsődleges hivatkozási modelljének.

Az OSI modell az összes olyan működést vagy feladatot tartalmazza, amely a hálózatok közötti kommunikációhoz társul, nem csak azokat melyek a TCP/IP protokollokra vonatkoznak. Összehasonlítva a TCP/IP modellel, melynek csak négy rétege van, az OSI modell a feladatokat még speciálisabb hét csoportba szervezi. Ezt követően a hét OSI réteg mindegyikéhez egy feladat, vagy a feladatok csoportja kerül hozzárendelésre.

A protokollkészlet lényege a fontos feladatok elkülönítése és megszervezése. A feladatok elkülönítése minden réteg számára lehetővé teszi a protokollkészletben, hogy a másikaktól függetlenül működjön. Például lehetséges az, hogy egy webhely otthonról a kábelmodemre csatlakoztatott laptop számítógépről, vagy vezeték nélküli kapcsolatot használó laptopról vagy egy web-képes mobiltelefonról legyen elérhető. Az alkalmazási réteg akadálytalanul működik tekintet nélkül arra, hogy az alsóbb rétegek milyen módon működnek.

Ugyanígy az alsóbb rétegek is akadálytalanul működnek. Például egy Internet csatlakozás kielégítően működik, ha olyan alkalmazások széles köre fut egyidőben mint az e-mail, a web böngészés, IM és zeneletöltés.



Fizikai réteg

- Meghatározza a hálózati berendezéseken keresztül történő adatküldés fizikai eszközeit.
- Interfész a hálózati közeg és az eszközök között.
- Meghatározza az optikai, elektromos illetve mechanikai jellemzőket.

Adatkapcsolati réteg

- Eljárásokat határoz meg a kommunikációs kapcsolatok működéséhez.
- Észleli és javítja a keretküldésből eredő hibákat.

Hálózati réteg

- Irányítja a csomagokat az egyedi hálózati eszköz címekkel összhangban.

Szállítási réteg

- Kezeli az üzenetek végponttól végpontig terjedő kézbesítést a hálózaton.
- Képes megbízható és sorrendhelyes csomagkézbesítést végezni a hibajavítási és áramlásellenőrzési mechanizmusoknak köszönhetően.

Viszony réteg

- Kezeli a felhasználói munkameneteket és párbeszédeket.
- Karbantartja a rendszerek közötti logikai kapcsolatokat.

Megjelenítési réteg

- Szabványosítja a felhasználói adatformátumokat a különböző típusú rendszerek közötti felhasználhatóság céljából.
- Kódolja és dekódolja a felhasználói adatokat; titkosítja illetve visszafejti a titkosított adatokat; betömöríti és kitömöríti az adatokat.

Alkalmazási réteg

- Interfészt határoz meg a szoftver alkalmazás és a hálózati kommunikációs feladatok között.
- Szabványosított szolgáltatásokat nyújt, például rendszerek között állományok átvitelére.

A Packet Tracer (PT) program egy olyan grafikus interfész, mely szimulált adatok két állomás között továbbításának megtekintését teszi lehetővé. Protokoll adategységeket (Protocol Data Unit, PDU) használ a hálózati forgalom kereteinek szemléltetésére és az OSI modell megfelelő szintjén kijelzi a protokoll információkat.

Az ábrán a web ügyfél kérését fogadja a web kiszolgálón levő Ethernet NIC. Az alábbi indormáció látható az OSI modell alsó 1-4 rétegénél.

1. réteg (Fizikai): Fast Ethernet port

2. réteg (Adatkapcsolati): Ethernet MAC címek

3. réteg (Hálózati):IP címek

4. réteg (Szállítási): TCP portszámok

7. Vezeték nélküli technológiák

7.1 Vezeték nélküli technológia

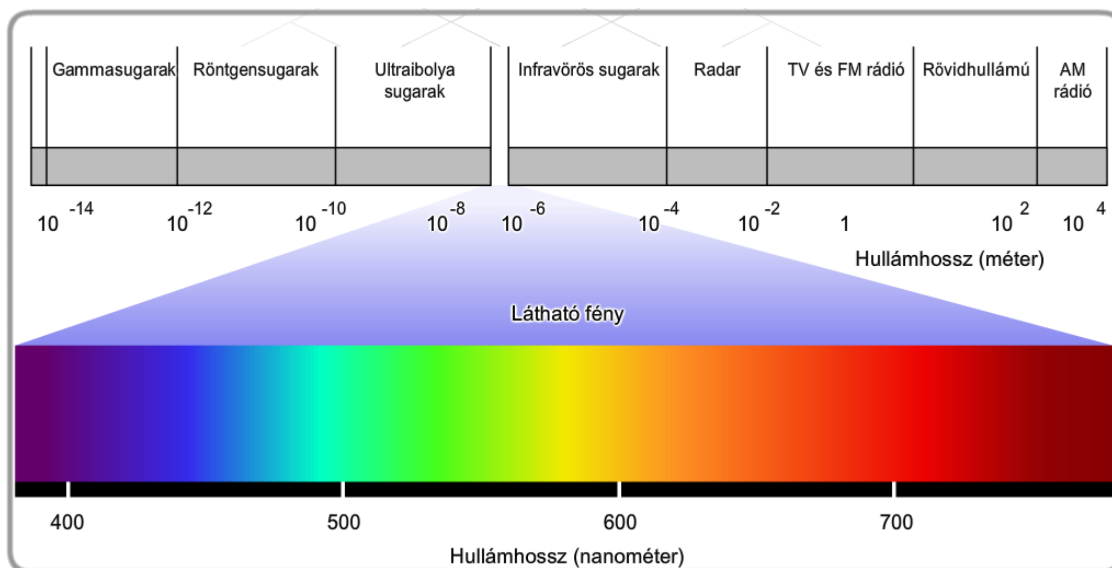
7.1.1 Vezeték nélküli technológiák és eszközök

A vezetékes hálózatokon kívül számos olyan technológia létezik, mely lehetővé teszi az eszközök közötti átvitelt kábelek használata nélkül. Ezeket vezeték nélküli technológiáknak nevezzük.

A vezeték nélküli eszközök elektromágneses hullámokat használva cserélik az információkat egymás közt. Egy elektromágneses hullám ugyanaz a közeg, mint amely a rádiójeleket is szállítja az éteren keresztül.

Az elektromágneses frekvencia spektrumba tartoznak a rádiós és televíziós műsorszórások frekvenciái, a látható fény, a röntgen és a gamma sugarak is. Ezek közül mindegyik külön hullámhossz tartománnyal és megfelelő energiaszinttel rendelkezik, ahogy az ábrán is látható.

Bizonyos típusú elektromágneses hullámok nem alkalmasak adatátvitelre. A frekvenciatartomány más részei állami szabályozás alatt vannak, és használatuk különféle szervezetek számára engedélyezett meghatározott tevékenységek ellátására. A tartomány bizonyos részeit közhasználatra tartják fenn, anélkül, hogy engedélyekhez kötnék használatukat. A nyilvános vezeték nélküli kommunikációra használt leggyakoribb hullámhosszok közé tartozik, az Infravörös és Rádiófrekvenciás (RF) tartomány.



Infravörös

Az Infravörös (IR) kommunikáció viszonylag alacsony energiaszintű, és jelei nem képesek áthatolni falakon vagy egyéb akadályokon. Ennek ellenére gyakran használják olyan eszközök közötti kapcsolat létrehozására és adatmozgatásra, mint személyes digitális titkár (Personal digital Assistent, PDA) és PC-k. Az eszközök közötti információcseréhez az IR egy infravörös közvetlen hozzáférésként (Infrared Direct Access, IrDA) ismert különleges kommunikációs portot használ. Az IR csak pont-pont típusú kapcsolatot tesz lehetővé.

Gyakran IR-t használnak a távirányítók, a vezeték nélküli egerek és a billentyűzetek is. Általában kis hatótávolságú, rálátást igénylő kommunikációra használják. Mindamellett reflexiós megoldásokkal az IR jelek hatóköre kiterjeszthető. Nagyobb távolságok esetén, magasabb frekvenciájú elektromágneses hullámok használatára van szükség.

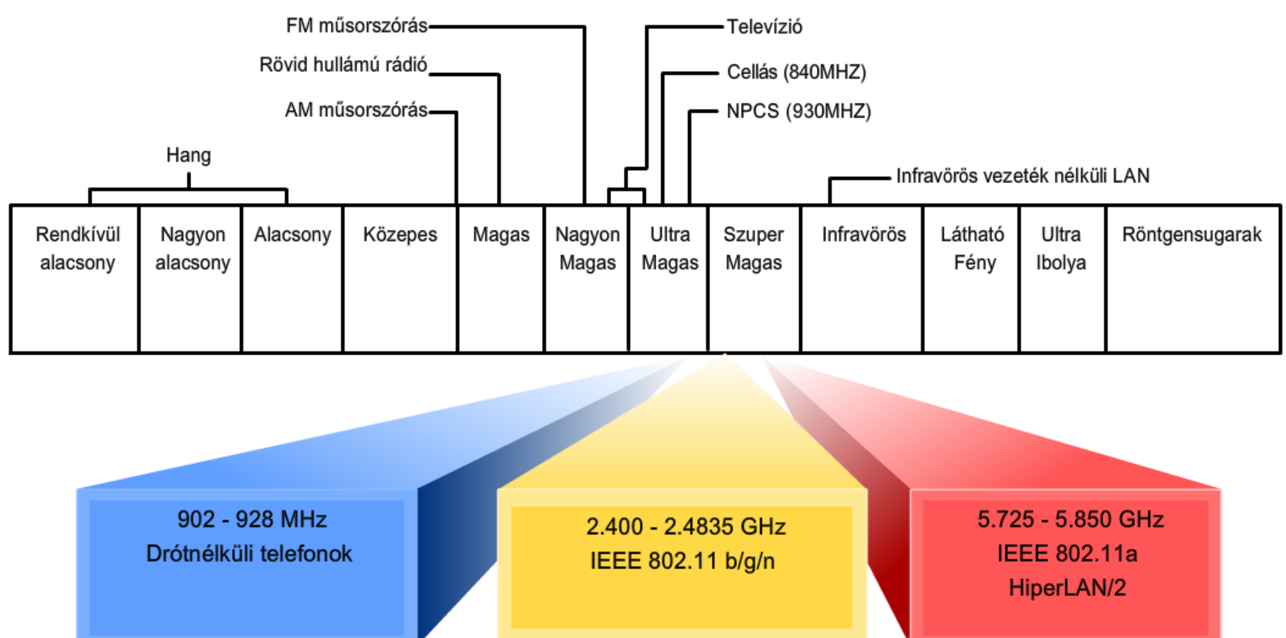
Rádió frekvencia (RF)

A rádió frekvenciás hullámok képesek áthatolni a falakon és más akadályokon, valamint az IR-hez képest jóval nagyobb a hatótávolságuk.

A rádiófrekvenciás (RF) tartomány bizonyos részeit szabadon használható eszközök működésére tartják fenn, ilyenek például a zsinór nélküli telefonok, vezeték nélküli helyi-hálózatok és egyéb számítógépes perifériák. Ilyen frekvenciák a 900 MHz, 2.4 és 5 GHz-es sávok. Ezen frekvenciák az Ipari, Tudományos és Orvosi sávokként (ISM) ismertek, és csekély megszorítások mellett használhatóak.

A Bluetooth egy kommunikációs technológia, mely a 2.4 GHz-es sávon működik. Korlátozott sebességű, és rövid hatótávolságú, de megvan az az előnye, hogy egyidejűleg több eszköz kommunikációját teszi lehetővé. Utóbbi előnyös tulajdonsága emelte a Bluetooth technológiát az Infravörös fölé, a számítógépes perifériák (nyomtatók, egerek és billentyűzetek) kapcsolatainak létrehozása esetében.

Egyéb technológiák, melyek a 2.4 és 5 GHz-es frekvenciákat használják, a különböző IEEE 802.11-es szaványoknak megfelelő modern vezeték nélküli hálózatok (WLAN). Abban különböznek a Bluetooth-tól, hogy magasabb teljesítményszinten továbbítanak, mely nagyobb hatótávolságot biztosít számukra.



7.1.2 A vezeték nélküli technológiák előnyei és korlátai

A vezeték nélküli hálózatok némely esetben előnyösebbek a hagyományos vezetékes hálózatokkal szemben.

Az egyik fő előnyük, hogy bárhol és bármikor lehetővé teszik a hálózati kapcsolódást. A vezeték nélküli hálózatok széleskörű megvalósítása a nyilvános helyeken, melyeket forrópontoknak (hotspot) hívunk, lehetővé teszi az emberek számára, hogy könnyen csatlakozzanak az Internetre, adatokat töltsenek le, levelet váltsanak és állományokat küldjenek egymásnak.

A vezeték nélküli hálózatok telepítése meglehetősen könnyű és olcsó. A otthoni és üzleti felhasználású WLAN eszközök ára folyamatosan csökken. Az árak csökkenése ellenére, ezen eszközök adatátviteli sebessége és képességük egyre növekszik, lehetővé téve a még gyorsabb és megbízhatóbb vezeték nélküli kapcsolatokat.

A vezeték nélküli technológia lehetővé teszi a hálózatok könnyű bővíthetőségét, a kábeles kapcsolatok okozta hátrányok nélkül. Az új és visszalátogató ügyfelek könnyen és gyorsan tudnak kapcsolódni.

A vezeték nélküli technológia előnyei és korlátai

- **Hordozhatóság** - egyszerű csatlakozást tesz lehetővé helyhez kötött és változó helyzetű ügyfelek számára.
- **Skálázhatóság** - egyszerűen bővíthető több felhasználó fogadása és a lefedettségi terület bővítése esetén
- **Rugalmasság** - bárhol, bármikor kapcsolódhatunk.
- **Költség megtakarítások** - A berendezések költsége folyamatosan csökken a technológia kiforrásával.
- **Rövid telepítési idő** - egyetlen eszköz felszerelése számos felhasználó kapcsolódását teszi lehetővé.
- **Megbízhatóság a mostoha körülményekben** - egyszerűen beüzemelhetőek a veszélyes és ellenséges környezetekben is.

A vezeték nélküli hálózatok előnyei és rugalmassága ellenére korlátaival és használatának kockázatával is számolnunk kell.

Először is, a Vezeték nélküli LAN (WLAN) technológiák a rádiófrekvenciás spektrum szabadon használható sávjait használják. Mivel e sávok használata nem szabályozott, számos eszköz üzemel ezeken a frekvenciákon. Ennek eredményeképpen ezek a frekvenciasávok nagyon zsúfoltak, és a különböző eszközök jelei gyakran zavarják egymást. Ezen kívül számos eszköz, mint például a mikrohullámú sütők vagy zsinórnélküli telefonok használhatják ezeket a sávokat, és interferálhatnak a WLAN kommunikációval.

Másodszor, a vezeték nélküli hálózatok fő problémája a biztonság. A WLAN-ok könnyű hálózati hozzáférést biztosítanak, amelyet az adatoknak sugárzással törénő továbbítása tesz lehetővé. Ez a tulajdonsága azonban korlátozza a vezeték nélküli technológia által nyújtott bitonság mértékét is. Bárki megfigyelheti a kommunikációs adatfolyamot annak ellenére, hogy nem neki szánták. E biztonsági problémákra válaszul, a vezeték nélküli átvitel védelme érdekében különböző technikákat fejlesztettek ki, például titkosítás és hitelesítés.

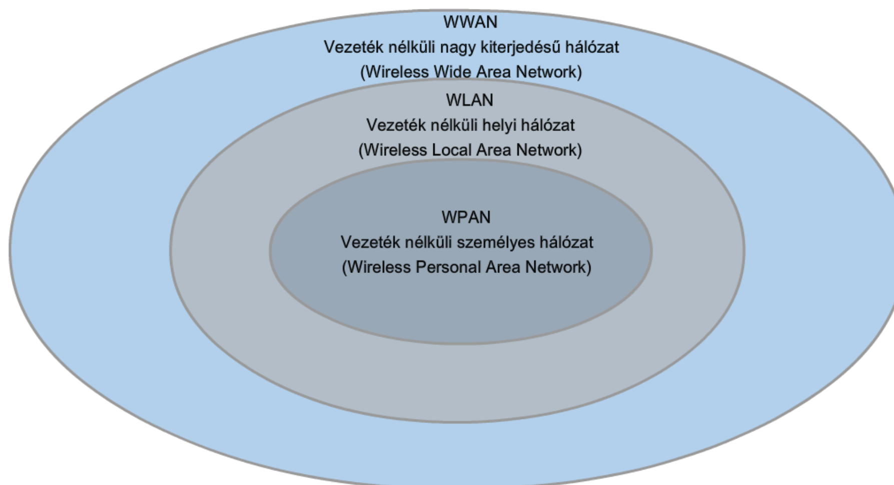
A vezeték nélküli technológia korlátai

- **Interferencia** - A vezeték nélküli technológia érzékeny a más elektromágneses erőteret keltő eszközöktől származó interferenciára. Ilyen eszközök például: zsinór nélküli telefonok, mikrohullámú sütők és más WLAN eszközök.
- **Hálózati és adatvédelem** - A WLAN technológiát az átvitelre kerülő adatok hozzáférésére és nem azok védelmére tervezték. Mindezek miatt, védtelen bejáratot biztosíthat a vezetékes hálózatba.
- **Technológia** - A vezeték nélküli hálózati technológia folyamatosan fejlődik. A WLAN technológia jelenleg nem biztosítja a vezetékes hálózatok által nyújtott sebességet és megbízhatóságot.

7.1.3 A vezetéknélküli hálózatok típusai és kötötségei

A vezeték nélküli hálózatok három fő csoportba sorolhatók: vezeték nélküli személyi hálózatok (WPAN), vezeték nélküli helyi hálózatok (WLAN) és vezeték nélküli nagy kiterjedésű hálózatok (WWAN).

E csoportosítás ellenére, nehéz meghatározni egy-egy vezeték nélküli hálózati megvalósítás hatókörét. Ennek oka, hogy a vezetékes hálózatokkal ellentétben, a vezeték nélküli hálózatoknak nincsenek pontosan meghatározott határai. A vezeték nélküli átvitel hatótávolságát számos tényező befolyásolja. Egyaránt érzékenyek a természetes és mesterséges eredetű zavarásokra. A hőmérséklet és páratartalom ingadozásai jelentősen befolyásolják a lefedettségi terület nagyságát. A vezeték nélküli környezetben található akadályok is csökkentik a hatótávolságot.



WPAN

A WPAN a legkisebb méretű hálózattípus, melyet általában olyan perifériális eszközök számítógéphez való csatlakoztatására használnak, mint például egerek, billentyűzetek és PDA-k. Ezen eszközök mindegyike kizárólag egy állomáshoz csatlakozik, és általában IR vagy Bluetooth technológiát használ.

WLAN

A WLAN-t általában a vezetékes helyi hálózatok határainak kiterjesztése érdekében használják. A WLAN RF technológiát használ, és megfelel az IEEE 802.11-es szabványoknak. Számos felhasználó számára teszi lehetővé a vezetékes hálózathoz való csatlakozást egy hozzáférési pontként (Acces Point, AP) ismert eszközön keresztül. A hozzáférési pont kapcsolatot biztosít a vezeték nélküli állomások és az Ethernet kábeles hálózat állomásai között.

WWAN

A WWAN hálózatok óriási méretű területeken biztosítanak lefedettséget. Ilyenek például a mobiltelefonos hálózatok. Olyan technológiákat használnak, mint a kódosztásos többszörös hozzáférés (Code Division Multiple Access, CDMA) vagy a Mobil kommunikáció globális rendszere (Global System for Mobile Communication, GSM), melyek használatát gyakran kormányzati szervek szabályozzák.

	WPAN	WLAN	WWAN
Értékelési szintek	Bluetooth v2.0+ EDR**	IEEE802.11 a/b/g/n, HiperLAN, HiperLAN2	GSM, GPRS, CDMA
Sebesség		1-540 Mbps	10-384 Kbps
Hatótávolság	Kicsi	Közepes	Nagy
Alkalmazások	Egyenrangú állomások hálózata Eszköztől eszközig	Otthoni, kisvállalati és nagyvállalati hálózatok	PDA-k, mobiltelefonok telefonok, mobiltelefonos elérés

** az EDR megnövelt adatátviteli sebességet (Enhanced Data Rate) jelent

Az újabb technológiáknak köszönhetően a sebesség és a hatótávolság folyamatosan növekszik.

7.2 Vezeték nélküli LAN-ok

7.2.1 Vezeték nélküli LAN-szabványok

Számos szabványt fejlesztettek ki annak érdekében, hogy a vezeték nélküli eszközök kommunikálni tudjanak egymással. Ezek meghatározzák a használt frekvencia tartományt, az adatátviteli sebességet, az információátvitel módját, stb.. A vezeték nélküli technikai szabványok létrehozásáért felelős elsődleges szervezet az IEEE.

Az IEEE 802.11-es szabvány határozza meg a WLAN környezeteket. Négy fő ajánlása létezik az IEEE 802.11 szabványnak, mely különböző jellemzőket ad meg a vezeték nélküli kommunikáció számára. A jelenleg létező ajánlások a 802.11a, 802.11b, 802.11g és 802.11n (a 802.11n a szöveg írásának idején még nem jóváhagyott). Összefoglaló néven, ezeket a technológiákat Wi-Fi-nek (Wireless Fidelity) nevezzük.

Egy másik szervezet, melyet Wi-Fi Szövetség néven ismerünk, a különböző gyártók WLAN eszközeinek teszteléséért felelős. Egy eszközön szereplő Wi-Fi embléma azt jelenti, hogy az eszköz megfelel a szabványoknak és képes más, ugyanezen szabványt használó eszközökkel való együttműködésre.

802.11a:

- Az 5 GHz-es frekvencia tartományt használja.
- Nem kompatibilis a 2.4 GHz-es sávot használó 802.11 b/g/n eszközökkel.
- Hatótávolsága nagyjából a 802.11 b/g hálózatok hatótávolságának 33%-a.
- Más technológiákhoz képest viszonylag költségesebb a megvalósítása.
- Egyre nehezebb 802.11a-nak megfelelő eszközt találni.

802.11b:

- A 2.4 GHz-es technológiák első képviselője.
- Maximális adatátviteli sebessége 11 Mbit/s.
- Beltérben maximálisan 46 méter (150 láb), kültéren 96 méter (300 láb) a hatótávolsága.

802.11g:

- 2,4 GHz-es technológia
- 54 Mbit/s a maximális adatátviteli sebessége
- Hatótávolsága a 802.11b-val megegyezik
- Felülről kompatibilis a 802.11b-vel

802.11n:

- A legújabb, fejlesztés alatt álló szabvány
- 2,4 GHz-es technológia (a szabvány tervezet az 5 GHz támogatását is említi)
- Megnövekedett hatótávolsággal és átbocsátóképességgel rendelkezik.
- Felülről kompatibilis a meglévő 802.11g és 802.11b eszközökkel (a szabványtervezet a 802.11a támogatását is megemlíti)

Gyakori IEEE WLAN szabványok

Szabvány	Kibocsátás dátuma	Frekvencia	Adatátviteli sebesség (Max)	Maximális hatótávolság*
802.11	1997 Július	2.4 GHz	2 Mbit/s	nem definiált
802.11a	1999 Október	5 GHz	54 Mbit/s	50 m
802.11b	1999 Október	2.4 GHz	11 Mbit/s	100 m
802.11g	2003 Június	2.4 GHz	54 Mbit/s	100 m
**802.11n	1.06-os tervezet elfogadva 2006 November 2.0 tervezet jóváhagyva 2007 Március	2.4 GHz vagy 5 GHz	540 Mbit/s	250 m

*Maximális hatótávolság - Ez az érték széles tartományban változhat. ~ A 802.11n szabvány még csak tervezetként létezik és az értékek változhatnak.

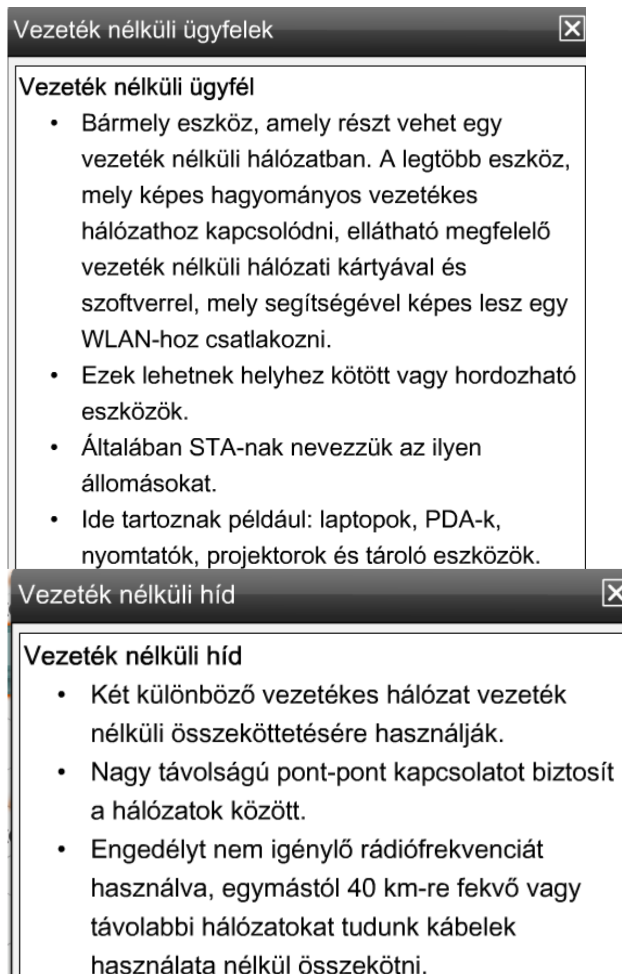
7.2.2 WLAN összetevők

Mihelyt egy szabványt elfogadnak, alapvető fontosságú, hogy a WLAN minden összetevője megfeleljen, vagy legalább kompatibilis legyen vele. Ez számos WLAN összetevőt érint, köztük a következőket: vezetéknélküli ügyfél vagy ún. STA, hozzáférési pont (AP), vezeték nélküli híd és antenna.

Hozzáférési pont

- A vezetékes és vezeték nélküli hálózatok közötti hozzáférés vezérlésért felelős. Tehát lehetővé teszi a vezeték nélküli ügyfelek számára, hogy hozzáférjenek a vezetékes hálózathoz és fordítva.
- Átviteli közeg átalakítóként működik, fogadja a vezetékes hálózat Ethernet kereteit és 802.11-nak megfelelő keretté alakítja, mielőtt továbbítja őket a WLAN-ra.

- A WLAN-ból érkező 802.11-es keretket fogadja, és Ethernet keretekké alakítja, mielőtt a vezetékes hálózatra helyezi őket.
- A hozzáférési pontok korlátozott területen biztosítanak hozzáférést, melyet vezeték nélküli cella vagy alapvető szolgáltatáskészletként (Basic Service Set (BSS)) ismerünk.



Antennák

Az AP-k és vezeték nélküli hidak esetében használják.

- Megnövelik a vezeték nélküli eszköz által kibocsátott jelek erősségét.
- Fogadják más eszközök, például STA-k jeleit.
- Az antennák által okozott jelerősség növekedést más néven erősítésnek nevezzük.
- A nagyobb erősítés rendszerint megnövekedett hatótávolságot jelent.

Az antennákat, a jelek sugárzásának a módja alapján osztályozzuk. Az irányított antennák egy irányba koncentrálják a jelek energiáját. Az irányítatlan antennákat arra tervezték, hogy minden irányba azonos erősséggel sugározzanak.

A jelek egy irányba való koncentrálásával, az irányított antennák nagy átviteli távolság elérésére képesek. Az irányított antennákat általában áthidalási problémák esetén használják, míg az irányítatlan antennákat a hozzáférési pontoknál (AP) találjuk meg.

7.2.3 WLAN-ok és az SSID

Egy Wi-Fi hálózat építésekor, fontos tényező, hogy az egyes összetevők a megfelelő WLAN-hoz csatlakozzanak. Erről a Szolgáltatáskészlet azonosító (Service Set Identifier, SSID) használatával gondoskodhatunk.

Az SSID érzékeny a kis és nagy betűkre, maximum 32 alfanumerikus karakterből áll. A WLAN-ban küldött minden keret fejlécében megtalálható. Az SSID-t arra használjuk, hogy a vezeték nélküli eszközöknek megmondjuk, melyik WLAN-hoz tartoznak és mely más eszközökkel kommunikálhatnak.

Tekintet nélkül arra, hogy milyen típusú WLAN kiépítésről van szó, a kommunikáció érdekében a WLAN minden vezeték nélküli eszközét ugyanarra az SSID-re kell beállítani.

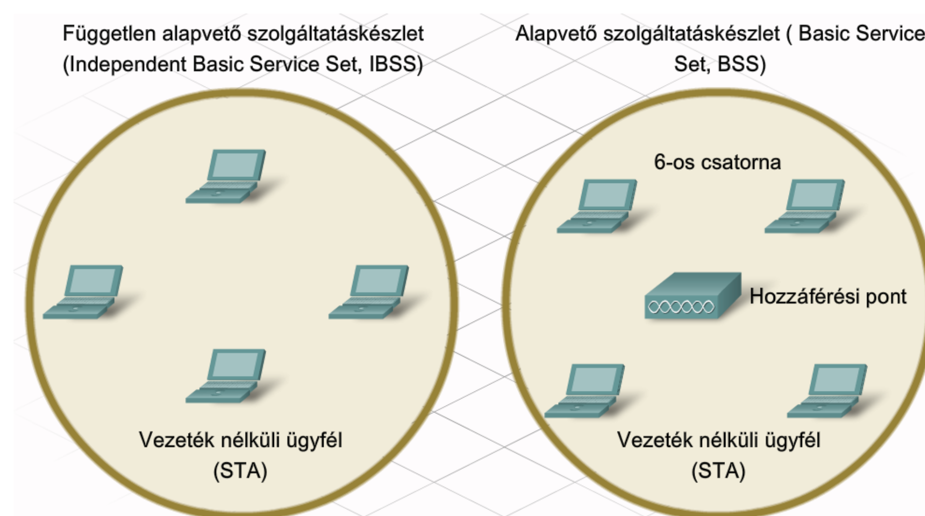
Alapvetően két különböző WLAN kiépítési forma létezik: Ad-hoc és infrastruktúrális mód.

Ad-hoc

A vezeték nélküli hálózatok legegyszerűbb formája, amikor két vagy több vezeték nélküli állomást kapcsolunk össze egyenrangú hálózatot létrehozva. Az ilyen hálózatokat ad-hoc vezeték nélküli hálózatoknak nevezzük, és hozzáférési pontot (AP) nem tartalmaznak. Egy ad-hoc hálózat minden állomása a hálózat egyenrangú résztvevője. A hálózat által lefedett terültet Független Alapvető Szolgáltatáskészletként (Independent Basic Service Set, IBSS) ismert. Az egyszerű ad-hoc hálózatokkal az eszközök állományokat és egyéb információkat cserélhetnek anélkül, hogy hozzáférési pont (AP) vásárlásának költségeivel és konfigurálásának bonyolultságával számolni kellene.

Infrastruktúrális mód

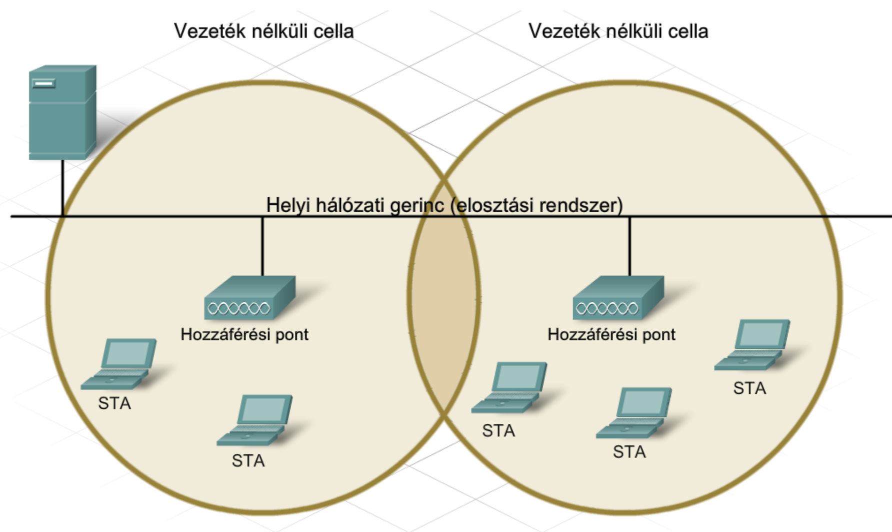
Bár az ad-hoc szervezés megfelelő lehet kisebb hálózatok esetén, nagyobb hálózatoknál egy önálló eszköz alkalmazása szükséges a vezeték nélküli cellában zajló kommunikáció irányításához. Ezt a szerepet a hozzáférési pont látja el, amely eldönti, ki és mikor kommunikálhat. Az infrastruktúrális módként ismert szervezési eljárást az otthoni és az üzleti környezetekben egyaránt a leggyakrabban használják. Egy ilyen típusú vezeték nélküli hálózatban, az egyes STA-k nem képesek egymással közvetlenül kommunikálni. A kommunikációhoz minden eszköznek engedélyt kell kérnie az AP-től. Az AP irányít minden kommunikációt és törekszik arra, hogy minden STA-nak egyenlő joga legyen a közeghez való hozzáféréshez. Egy egyedüli AP által lefedett területet alapvető szolgáltatáskészletként (Basic Service Set, BSS) vagy cellaként ismerünk.



Az alapvető szolgáltatáskészlet (Basic Service Set, (BSS) a WLAN hálózatok legkisebb építőeleme. Egy AP által lefedett terület nagysága korlátozott. A lefedettségi terület kibővítéséhez több BSS is összeköthető egymással egy elosztórendszer (Distribution system, DS) használatával. Ezzel egy Extended Service Set (ESS) jön létre. Egy ESS több hozzáférési pontot használ. Az egyes AP-k különálló BSS-ben vannak.

Azért, hogy a cellák között a jelek elvesztése nélkül biztosítsuk kapcsolatot, az egyes BSS-ek között megközelítőleg 10% átfedésnek kell lennie. Ez lehetővé teszi az ügyfelek számára, hogy azelőtt csatlakozzanak a másik AP-hez mielőtt az első AP-ről lecsatlakoztak.

A legtöbb otthoni és kisvállalati környezet összesen egy BSS-ből áll. Azonban, ha az igényelt lefedett terület mérete és a kapcsolódni kívánó ügyfelek száma növekszik, akkor szükséges lehet egy ESS létrehozása.



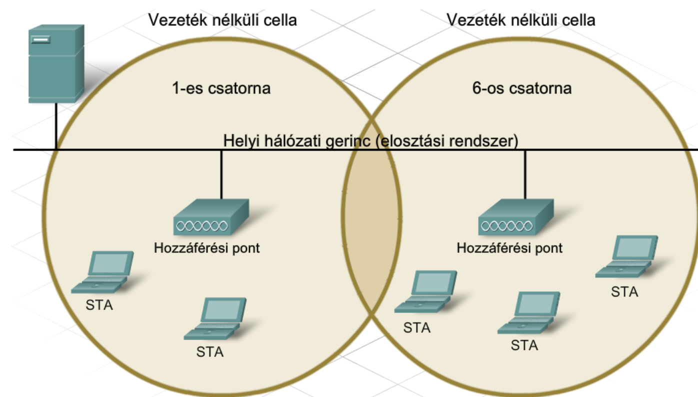
7.2.4 Vezeték nélküli csatornák

Ha egy IBSS, BSS vagy ESS területén belül a vezeték nélküli ügyfelek kommunikálnak egymással, a küldő és fogadó állomások közötti párbeszédet irányítani kell. Az egyik módszer, mely ezt megvalósítja, a csatornák használata.

A csatornák a rendelkezésre álló RF tartomány részekre bontásával jönnek létre. Az egyes csatornák különböző párbeszédek bonyolítására alkalmasak. Ez hasonló ahhoz, amikor több televíziós csatornát szolgáltatnak egyetlen átviteli közegen keresztül. Több hozzáférési pont képes egymáshoz közel üzemelni, amíg azok eltérő csatornát használnak a kommunikációra.

Sajnos egyes csatornák által használt frekvenciák átfedésben lehetnek mások által használt csatornákkal. A különböző párbeszédeknek egymást nem átfedő csatornákon kell zajlaniuk. A csatornák felosztása és száma a felhasználási területtől és a technológiától is függ. Egy bizonyos kommunikációra használt csatorna kiválasztása kézire illetve automatikusra állítható, olyan tényezőktől függően, mint a terhelés mértéke és a rendelkezésre álló áteresztőképesség.

Normál esetben minden egyes vezeték nélküli párbeszédhez különálló csatornákat használnak. Néhány újabb technológia képes a csatornák kombinálására, létrehozva egy szélesebb átviteli csatornát, amely nagyobb sávszélességget és megnövekedett adatátviteli sebességet biztosít.



Egy WLAN-on belül, a cellák közötti jól meghatározott határvonalak hiánya miatt lehetetlen az átvitel során fellépő ütközések észlelése. Ezért, olyan közeghozzáférési módszert kell használni a vezeték nélküli hálózatokban, amely biztosítja, hogy ne forduljanak elő ütközések.

A vezeték nélküli technológia az úgynevezett vivőérzékeléses többszörös hozzáférésű - ütközés elkerüléses (Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA) közeghozzáférési módszert használja. A CSMA/CA lefoglalja a párbeszédre használandó csatornát. Amíg a foglalás érvényben van, más eszköz nem adhat ugyanazon csatornán, így a lehetséges ütközések elkerülhetők.

Hogyan működik ez a foglalási folyamat? Ha egy eszköz egy bizonyos kommunikációs csatornát szeretne használni egy BSS-ben, először az AP engedélyét kell kérnie. Ezt a folyamatot küldéskérésként (Request to Send, RTS) ismerjük. Ha a kívánt csatorna elérhető, az AP a Küldésre kész (Clear to Send, CTS) választ adja a kliensnek, amely azt jelzi, hogy az eszköz használhatja a csatornát. Egy CTS válasz szórás formájában minden eszközhöz eljut a BSS területén. Így a BSS cella minden eszköze tudomást szerez arról, hogy csatorna jelenleg foglalt.

Miután a párbeszéd befejeződött, a csatornát lefoglaló eszköz egy másik üzenetet küld az AP-nek, melyet nyugtaként (Acknowledgement, ACK) ismerünk. Az ACK jelzi a hozzáférési pontnak, hogy a csatorna foglaltsága felszabadítható. Ezt az üzenetet a WLAN minden eszköze megkapja üzenetszórás formájában. A BSS cella minden eszköze fogadja az ACK üzenetet, tudomást szerezve arról, hogy a csatorna ismét elérhető.

7.2.5 Hozzáférési pont konfigurálása

Miután megtörtént a használandó vezeték nélküli szabvány kiválasztása, az eszközök elrendezése és a csatorna hozzárendelés is már kész, itt az ideje a hozzáférési pont (AP) konfigurálásának.

A legtöbb integrált forgalomirányító lehetőséget ad vezetékes és vezeték nélküli kapcsolódásra, és AP-ként is szolgál a hálózatban. Az olyan alapvető beállítások, mint a jelszavak, az IP címek és DHCP beállítások megegyeznek attól függően, hogy az eszközt vezetékes vagy vezeték nélküli állomás csatlakoztatására használjuk. Az olyan alapvető konfigurációs feladatokat, mint az alapértelmezett jelszó megváltoztatása, az AP éles hálózatba történő bekötése előtt kell elvégezni.

Ha egy integrált forgalomirányító vezeték nélküli funkcióját használjuk, olyan további beállítások szükségesek, mint a vezeték nélküli mód, az SSID és a használt csatorna konfigurálása.

Vezeték nélküli mód

A legtöbb otthoni AP többféle módot támogathat, leggyakrabban: 802.11b, 802.11g, 802.11n. Bár ezek mind a 2.4 GHz-es tartományt használják, más-más technológiát használnak a maximális áteresztőképesség eléréséhez. Az engedélyezett mód határozza meg, milyen típusú állomások csatlakozhatnak az AP-hez. Ha csak azonos típusú állomások csatlakoznak a hozzáférési ponthoz, állítsuk arra a módra, melyet az állomások használnak. Többféle típusú eszköz esetén állítsuk vegyes (mixed) módra a hálózatot. Mindegyik mód használata bizonyos mértékű többletterhelést okoz. A vegyes (mixed) mód beállításával a hálózati teljesítmény csökkenni fog az összes üzemmód támogatása által okozott többletterhelés miatt.

SSID

Az SSID-t a WLAN azonosítására használják. Az összes eszköznek, amely egy hálózatban szeretne működni, ugyanazon SSID beállítással kell rendelkeznie. Ahhoz, hogy az ügyfelek könnyen észleljék a hálózatot, a hozzáférési pontok szórásos üzenetekkel terjesztik az SSID-t. Lehetőség van az SSID szórásának kikapcsolására is. Ilyenkor azonban a vezeték nélküli ügyfeleknél kézzel kell beállítani ezt az értéket.

Vezeték nélküli csatorna

Az AP számára történő csatornaválasztásnak a környezetben működő más vezeték nélküli hálózatokhoz viszonyítva kell megtörténnie. A szomszédos BSS-eknek egymást nem átfedő csatornát kell használniuk az optimális áteresztőképesség biztosítása érdekében. Ma már a legtöbb AP esetén lehetőség van a kézi csatornabeállításra, vagy engedélyezhetjük az automatikus kiválasztást is, amely a legkevésbé leterhelt vagy a legnagyobb áteresztőképességű csatorna használatát teszi lehetővé.

Hálózati mód

Meghatározza a támogatandó technológia típusát. Például, **802.11b, 802.11g, 802.11n** vagy **Kevert mód**.

SSID

A WLAN hálózatok azonosítására használják. Minden olyan eszköznek, mely részese kíván lenni a WLAN hálózatnak ugyanazt az SSID-t kell használnia.

Szabványos csatorna

Meghatározza a kommunikációra használt csatornát. Alapértelmezés szerint, ez **Auto** (automatikus) üzemmódra van állítva hogy az optimális csatorna használatát biztosítsa az AP számára.

SSID szórás

Meghatározza, hogy az SSID üzenetszórással lesz-e hirdetve a hatókörön belüli összes eszköznek. Alapértelmezés szerint Enable (Bekapcsolva).

7.2.6 Vezeték nélküéi ügyfél konfigurálása

Vezeték nélküli állomásnak vagy STA-nak nevezünk minden olyan eszközt, amely tartalmaz valamilyen vezeték nélküli hálózati csatolót (NIC) és ennek működéséhez szükséges ügyfélprogramot. Az ügyfélszoftver teszi lehetővé, hogy a hardver a WLAN része legyen. STA-k közé tartozó eszközök például: PDA-k, laptopok, asztali PCk, nyomtatók, projektorok és Wi-Fi telefonok.



Ahhoz, hogy egy STA a WLAN-hoz csatlakozzon, az ügyfélprogram konfigurációjának meg kell egyeznie a hozzáférési pontéval. Ezek közé tartozik az SSID, a biztonsági beállítások, és a csatorna adatok, akkor ha nem automatikus csatorna kiválasztás van beállítva. Ezen beállítások az ügyfél kapcsolatát irányító kliens szoftverben kerülnek megadásra.

A használt ügyfélprogram lehet az eszköz operációs rendszerébe integrált vagy lehet különálló, letölthetö szoftver, melyet kizárólag bizonyos vezeték nélküli NIC kezelésére terveztek.

Beépitett vezeték nélküli segédprogramok

A Windows XP vezeték nélküli kliens szoftvere egy példa azokra a népszerű ügyfélprogramokra, melyet az eszköz operációs rendszere részeként mellékelnek. Ez az ügyfélprogram egy alapvető kezelőprogram, amely képes ellenőrizni a legtöbb vezeték nélküli ügyfélkonfigurációt . Felhasználóbarát és egyszerűvé teszi a kapcsolódási folyamatot.

A különálló vezeték nélküli szoftverek

Az olyan vezeték nélküli segédprogramokat, mint amiket a vezeték nélküli hálózati kártyákhoz is mellékelnek, úgy tervezték, hogy csak meghatározott hálózati csatolóval (NIC) működjön. Rendszerint a Windows XP beépített programjához képest továbbfejlesztett funkciókra képesek, többek között:

- **Kapcsolat információ** - megjeleníti a vezeték nélküli jel aktuális erősségét és minőségét
- **Profilok** - lehetővé teszik különböző vezeték nélküli hálózatokhoz egyedi beállítások megadását: SSID, csatorna száma, stb.
- **Helyszínek vizsgálata (Site Survey)** - lehetővé teszi a környék összes vezeték nélküli hálózatának észlelését.

Nem lehetséges, hogy a vezeték nélküli segédprogram és a Windows XP beépített programja egyszerre kezelje a hálózati kapcsolatokat. A legtöbb esetben a Windows XP integrált szoftvere megfelel az elvárásoknak. Ha több hálózati profilt kell létrehozni a különböző hálózatok számára, vagy speciális konfigurációs beállításokra van szükség, jobb ha a hálózati kártyához mellékelt programot használjuk.

Miután az ügyfél szoftvert beállítottuk, ellenőrizzük a kliens és az AP közötti kapcsolatot.

Nyissuk meg a vezeték nélküli kapcsolat információs ablakát, amely olyan információkat jelenít meg, mint a kapcsolat adatátviteli sebessége, a csatlakozás állapota és a használt csatorna. A kapcsolat információ menüpont, ha rendelkezésre áll, megjeleníti a vezeték nélküli jel erősségét és minőségét.

A kapcsolat ellenőrzéséhez győződjünk meg arról is, hogy továbbíthatóak-e az adatok. Az egyik leggyakrabban használt módszer az adatátvitel ellenőrzésére a Ping-teszt. Ha a ping-teszt sikeres, az adatátvitel lehetséges.

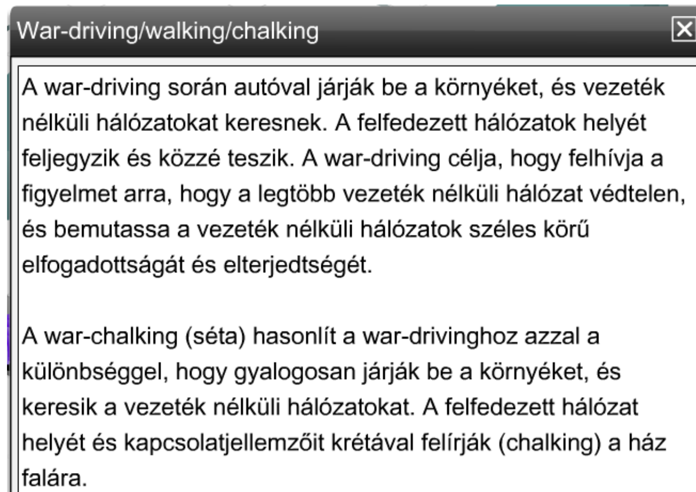
Ha a forrás és célhely között a teszt sikertelen, pingessük meg az AP-t a vezeték nélküli állomásról a kapcsolódás tényleges ellenőrzéséhez. Ha ez sem sikerül, a probléma az állomás és a hozzáférési pont között van. Ellenőrizzük a beállításokat és próbáljuk helyreállítani a kapcsolatot!

Ha a vezeték nélküli ügyfél sikeresen csatlakozott az AP-hez, próbáljuk tesztelni a következő ugrást az AP-től a célállomás felé vezető úton. Ha ez is sikeres, akkor a probléma valószínűleg nem az AP beállításaival van, hanem a célhoz vezető út valamelyik eszközével vagy magával a céleszközzel.

7.3 Hálózatbiztonsági megfontolások a vezetéknélküli LAN-nal kapcsolatban

7.3.1 Miért támadják a WLAN-okat?

A vezeték nélküli hálózatok egyik legnagyobb előnye, hogy az eszközök egyszerű és kényelmes csatlakozását teszik lehetővé. Sajnos a kapcsolódás egyszerűsége és annak ténye, hogy az információ a levegőn keresztül kerül átvitelre, sebezhetővé teszi hálózatunkat a behatolásokkal és támadásokkal szemben.



A vezeték nélküli kapcsolódás miatt, a támadónak nem szükséges fizikailag csatlakozni számítógépünkhöz vagy hálózatunk bármely eszközéhez. Lehetséges az, hogy egy támadó ráhangolódjon hálózatunk vezeték nélküli jeleire, épp úgy, mint amikor behangolunk egy rádióállomást.

A támadó a lefedettségi területen belül képes hozzáférni hálózatunkhoz. Miután bejutott, ingyen használhatja az Internet kapcsolatot, valamint kárt tehet a hálózathoz csatlakozó más számítógépek adataiban vagy ellophat személyes információkat.

A vezeték nélküli hálózatok sebezhetősége miatt a WLAN támadások elleni védekezés érdekében speciális biztonsági szolgáltatásokra és megvalósítási módszerekre van szükség. Ezek közé tartoznak a vezeték nélküli eszköz előzetes beállításakor elvégzendő egyszerű teendők ugyanúgy, mint a jóval fejlettebb biztonsági konfigurációk.

Az egyik egyszerű módszer egy vezeték nélküli hálózatba való bejutáshoz, ha tudjuk a hálózat nevét, az SSID-t.

A hálózathoz csatlakozó minden számítógépnek ismernie kell az SSID-t. Alapértelmezés szerint, a vezeték nélküli forgalomirányítók és hozáférési pontok a lefedettségi terület minden állomása felé szórják az SSID-t. Az SSID szórás bekapcsolásával, bármely vezeték nélküli ügyfél észlelheti és csatlakozhat a hálózathoz, ha nincsenek érvényben egyéb biztonsági beállítások.

Az SSID szórása kikapcsolható. Ha ki van kapcsolva, a hálózat létezése többé nem nyilvános. Bármely csatlakozni kívánó számítógépnek ismernie kell az SSID-t.

Továbbá, fontos az alapértelmezett beállítások megváltoztatása. A vezeték nélküli eszközök bizonyos beállításai előre konfiguráltak, például az SSID, jelszavak és az IP címek. Ezen alapértelmezett adatok használata egyszerűvé teszik egy támadó számára a hálózat azonosítását és az abba való behatolást.

Még ha az SSID szórás ki is van kapcsolva, elég valószínű, hogy valaki jól ismert SSID-kkel próbálkozva bejut hálózatunkba. Ezen kívül, ha az egyéb alapértelmezett beállítások, mint jelszavak és IP címek nem kerülnek megváltoztatásra, akkor a támadók hozzáférhetnek az AP-hez és változtatásokat eszközölhetnek rajta. Az alapértelmezett adatokat érdemes valamilyen biztonságosabb, egyedi értékre változtatni.

A fenti változtatások önmagukban nem védik meg hálózatunkat. Például az SSID-k titkosíttatlan szöveg formájában kerülnek átvitelre. Vannak olyan eszközök, amelyek képesek elfogni a vezeték nélküli jeleket és a titkosítattlanul küldött adatokat. Így, még ha az SSID szórását ki is kapcsoltuk és megváltoztattuk a gyári értékeket, a támadók a vezeték nélküli jeleket elfogva és feldolgozva ki tudják deríteni hálózatunk azonosítóját, és felhasználhatják a hálózathoz való csatlakozáshoz. Csak többféle módszer együttes alkalmazásával védhetjük meg WLAN-unkat.

7.3.2 Egy WLAN erésének korlátozása

A vezeték nélküli hálózat használata korlátozásának egyik módszere, hogy pontosan megmondjuk, mely eszközök csatlakozhatnak. Ezt a MAC-címek szűrésével érhetjük el.

MAC cím szűrés

A MAC cím szűrés a MAC címeket használja annak eldöntéséhez, hogy mely eszközök engedélyezettek a hálózat elérésére. Ha egy vezeték nélküli állomás megpróbál csatlakozni vagy társítást kezdeményezni egy AP-val, elküldi saját MAC cím információját. Ha a MAC cím szűrés be van kapcsolva, a vezeték nélküli forgalomirányító, illetve a hozzáférési pont megkeresi a kliens MAC címét egy előre létrehozott listában. Csak azon eszközök engedélyezettek a csatlakozásra, melyek MAC címeit előzetesen rögzítették a forgalomirányító adatbázisába.

Ha a MAC cím nem található a listában, akkor az eszköz nem csatlakozhat vagy veheti igénybe a hálózatot.

Ezzel a biztonsági módszerrel is van azonban néhány probléma. Az egyik, hogy a hálózathoz csatlakozni kívánó összes eszköz MAC címének rögzítve kell lennie az adatbázisban, mielőtt a csatlakozási próbálkozások megtörténnének. Ha egy eszköz nincs azonosítva az adatbázisban, akkor nem fog tudni csatlakozni. A másik probléma az, hogy a támadó felhasználhatja egy hozzáféréssel rendelkező, engedélyezett eszköz MAC címét.

7.3.3 Hitelesítás egy vezetéknélküli hálózatban

Egy másik módszer a csatlakozások szabályozásához a hitelesítés alkalmazása. A hitelesítés az a folyamat, mely során hitelesítési információk alapján dől el a belépés engedélyezése. Annak eldöntésére használják, hogy a kapcsolódni kívánó eszköz megbízható-e.

Jelszó és felhasználói név használata a hitelesítés leggyakoribb formája. Egy vezeték nélküli környezetben, a hitelesítési folyamat biztosítja a csatlakozó állomás megbízhatóságát, de a felülvizsgálati folyamat kissé eltérő módon zajlik. A hitelesítés folyamat, ha engedélyezve van, még azelőtt megtörténik, mielőtt az ügyfél beléphetne a WLAN-ba. Három különböző típusú vezeték nélküli hitelesítési módszer létezik: a nyílt hitelesítés, a PSK és az EAP.

Nyílt hitelesítés

Alapértelmezés szerint a vezeték nélküli eszközök nem igényelnek hitelesítést. Minden hálózati eszköz képes a társításra, tekintet nélkül arra, hogy melyek azok valójában. Minden hálózati eszköz

képes a csatlakozásra függetlenül attól, ki is valójában. A nyílt hitelesítést közhasznú hálózatok esetén érdemes alkalmazni, például amelyek iskolákban vagy éttermekben találhatóak. Akkor is használható, ha a hálózatba való belépés után más eszközökkel végezzük a hitelesítési eljárást.

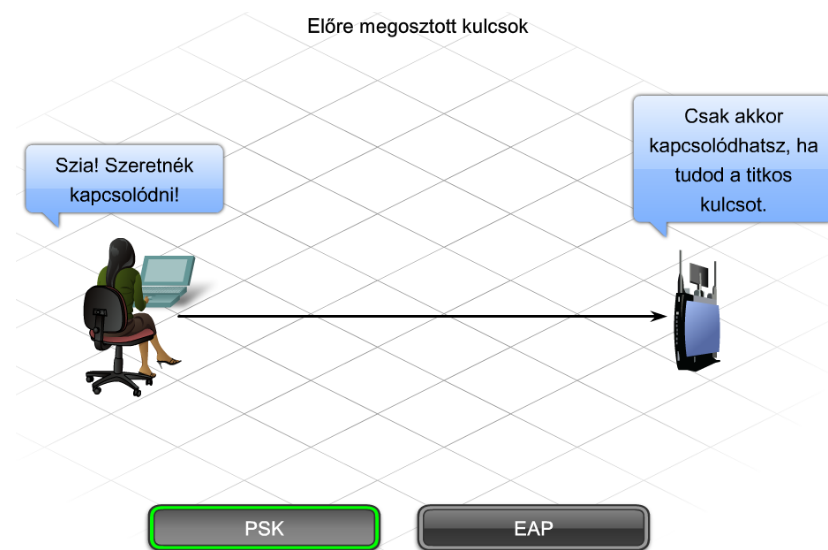
Előre megosztott kulcs (PSK)

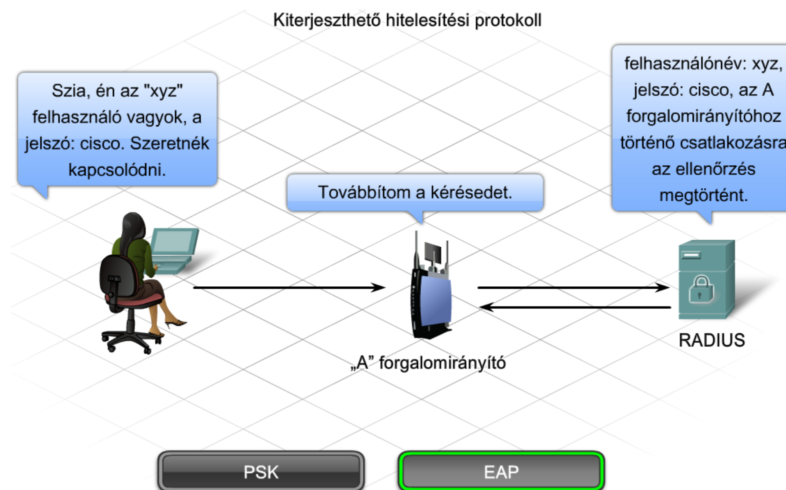
PSK használata esetén, az AP-n és az ügyfél eszközön ugyanazzt a kulcsot vagy titkos szót kell beállítani. Az AP egy véletlenül generált bájtsorozatot küld az ügyfélnek. Az ügyfél fogadja a bájtsorozatot, a kulcs alapján titkosítja (kódolja), és visszaküldi a hozzáférési pontnak. Az AP fogadja a kódolt üzenetet, és a saját kulcsát használva visszafejti (dekódolja). Ha a visszafejtett bájtsorozat megegyezik az eredetileg küldöttel, az ügyfél kapcsolódhat a hálózatra.

A PSK egyutas hitelesítést végez, azaz csak az állomás hitelesíti magát a hozzáférési ponton. A PSK nem hitelesíti az AP-t az ügyfél eszközön, és nem azonosítja az állomás tényleges felhasználóját sem.

Kiterjeszthető Hitelesítési Protokoll (EAP)

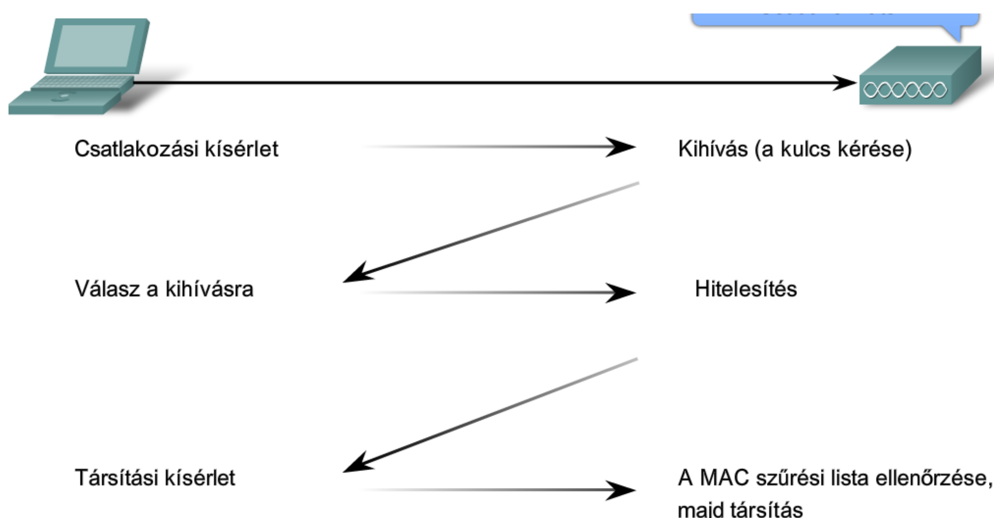
Az EAP kölcsönös vagy kétutas hitelesítést biztosít, és lehetővé teszi a felhasználó azonosítását is. Ha EAP-ot használó programot telepítettek egy állomásra, az ügyfél egy kiszolgáló oldali hitelesítő szerverrel kommunikál, mint például a távoli hitelesítés behívásos felhasználói szolgáltatás (Remote Authentication Dial-in User Service, RADIUS). Ez a kiszolgáló oldali szolgáltatás különválasztva működik a hozzáférési pontoktól és adatbázist tart fenn a hálózatot használni jogosult felhasználókról. Amikor EAP-ot használnak, a felhasználónak - nem csak az állomásnak - meg kell adnia az azonosítóját és a jelszavát, melyek érvényességét a RADIUS adatbázisban ellenőrzik. Ha az adatok érvényesek, a felhasználó hitelesítése sikeres.





Ha valamilyen hitelesítés be van állítva, a hitelesítés módjától függetlenül, az ügyfélnek előbb sikeresen át kell esnie a hitelesítésen, mielőtt az AP-al való társítási folyamat elkezdődne. Ha a hitelesítés és a MAC-cím szűrés egyaránt be van állítva, a hitelesítési folyamat zajlik le először.

Ha a hitelesítés sikeres, az AP ellenőrzi a MAC címet. Ha a cím érvényes, a hozzáférési pont az állomás táblájába teszi az ügyfél MAC címét. Az állomást ekkor tekintjük társítottnak a hozzáférési ponthoz (AP), és használhatja a hálózatot.



7.3.4 Titkosítás WLAN-on

A hitelesítés és a MAC cím szűrés megakadályozhatja a támadók hálózathoz való hozzáférését, de nem előzik meg az átvitt adatok elfogásának lehetőségét. Mivel egy vezeték nélküli hálózatnak nincsenek pontosan definiálható határai és az adatátvitel a levegőn keresztül történik, egy támadó számára egyszerű a vezeték nélküli keretek elfogása vagy más néven lehallgatása (sniffing). A titkosítási folyamat az adatok átalakítását jelenti, így az elfogott információk használhatatlanok lesznek.

Vezetékessel egyenértékű protokoll (Wired Equivalency Protocol, WEP)

A Vezetékessel Egyenértékű titkosítási Protokoll (WEP) egy fejlett biztonsági lehetőség, mely a levegőben áthaladó hálózati forgalom titkosítását végzi. A WEP előre beállított kulcsok használatával kódolja és fejti vissza az adatokat.

A WEP-kulcsokat szám- vagy betűsorozat formájában használják, többnyire 64 vagy 128 bit hosszúsággal. Némely esetben a 256 bit hosszú kulcsok is támogatottak. Ezen kulcsok létrehozásának és beírásának egyszerűsítése végett számos eszköz felkínálja a Jelmondat (Passphrase) lehetőségét. A passphrase segítségével könnyen észben tarthatunk egy szót vagy kifejezést, melyet a kulcsok automatikus létrehozásához használhatunk.

Annak érdekében, hogy a WEP működjön, a hozzáférési pontnál és az összes engedélyezett állomáson ugyanazon WEP kulcsot kell megadni. Ezen kulcs nélkül, az eszközök nem tudnák értelmezni az átvitelt.

A WEP egy nagyszerű mód arra, hogy megakadályozzuk a támadókat a jelek elfogásában. Azonban megvannak a WEP hátrányai is, például, hogy az összes WEP állomáson statikus (állandó) érvényű kulcsokat használ. Léteznek olyan alkalmazások, melyek segítségével a támadók kideríthetik a WEP kulcsot. Ezek a programok hozzáférhetőek az Interneten. Miután a támadó kinyerte a kulcsot, teljes hozzáférést szerez az összes továbbított információhoz.

A sebezhetőség elkerülésének egyik módja a WEP kulcsok gyakori megváltoztatása. A másik módszer egy jóval fejlettebb és biztonságosabb titkosítási eljárás, a Wi-Fi Védett Hozzáférés (WPA) alkalmazása.

Wi-Fi Védett Hozzáférés (WPA)

A WPA is 64 és 256 bit közötti hosszúságú kulcsokat használ. A WPA azonban a WEP-pel ellentétben új, dinamikus kulcsokat hoz létre minden alkalommal, amikor egy állomás kapcsolódik a hozzáférési ponthoz. Éppen ezért a WPA jóval biztonságosabb, mint a WEP, mivel sokkal nehezebb feltörni.

7.3.5 Forgalomszűrés egy WLAN-on

Annak szabályozásán kívül, hogy ki fér hozzá a WLAN-hoz, és ki használhatja fel a továbbított adatokat, fontos, hogy a WLAN-on keresztül továbbított hálózati forgalom típusát is szabályozni lehessen. Ezt forgalomszűrés segítségével valósítják meg.

A forgalomszűrés letiltja mind a hálózatba belépő, mind a hálózatot elhagyni kívánó nemkívánatos forgalmat. A szűrést az AP végzi el, miközben a forgalom áthalad rajta. A szűrés arra használható, hogy bizonyos forrásállomás felől jövő vagy célállomás felé igyekvő forgalmat MAC vagy IP címek alapján kiszűrjünk. Ezen kívül számos alkalmazás működését blokkolhatjuk a megfelelő portszámok letiltásával. Azáltal, hogy eltávolítjuk a nemkívánatos, haszontalan és gyanús adatforgalmat a hálózatból, jóval nagyobb sávszélesség áll rendelkezésre a fontos adatok átvitelére, ami a WLAN teljesítményének növekedését eredményezi. Például, a forgalomszűrést használhatjuk arra, hogy letiltsunk minden olyan Telnet forgalmat, amely egy meghatározott számítógépre, például egy hitelesítő kiszolgálóra irányul. Bármely próbálkozás, amely telnet segítségével próbálja elérni a hitelesítő szervert, gyanús hálózati forgalomnak számít és le lesz tiltva.

7.4 Egy integrált AP és egy vezeték nélküli ügyfél konfigurálása

7.4.1 WLAN tervezése

Egy vezeték nélküli hálózat megvalósításakor a telepítést gondos tervezésnek kell megelőznie. Ezek közé tartozik:

- A használandó vezeték nélküli szabvány meghatározása
- Az eszközök leghatékonyabb elhelyezésének meghatározása
- Egy telepítési és biztonsági terv elkészítése
- A vezeték nélküli eszközök firmware-jének mentési és frissítési stratégiája

Vezeték nélküli szabványok

Tekintettel kell lennünk számos tényezőre, mielőtt egy WLAN szabvány használata mellett döntenénk. A legfontosabb tényezők közé tartozik: sávszélességi követelmények, lefedettségi területek, meglévő hálózatok szabványa, költségek. Ezen információkat a végfelhasználói igények megismerésével gyűjthetjük össze.

- Ennek legegyszerűbb formája, ha kérdéseket intézünk a felhasználók felé.
- Jelenleg mekkora sávszélességet igényelnek a hálózaton futtatott programok?
- Összesen hány felhasználó használná a WLAN-t?
- Mekkora lefedettségi területre van szükség?
- Milyen a meglévő hálózati kiépítés?
- Mekkora a költségvetés?

A BSS cellában elérhető maximális sávszélességet az adott BSS felhasználói között meg kell osztani. Még ha a használt alkalmazások nem is igényelnek nagy sávszélességet, egy nagyobb sebességű technológia valamelyikére lehet szükség, ha egyidőben több felhasználó is csatlakozik a hálózathoz.

A különböző szabványok eltérő méretű lefedettségi területet biztosítanak. A 802.11 b/g/n technológiák által használt 2,4 GHz-es jelek nagyobb hatótávolságúak, mint a 802.11a szabvány 5 GHz-es jelei. Ezért a 802.11 b/g/n szabványok nagyobb területű BSS-ek kialakítására alkalmasak. Emiatt kevesebb eszközt kell beépíteni, ami alacsonyabb megvalósítási költséggel jár.

A létező hálózatok ugyancsak befolyásolják a telepítésre kerülő WLAN szabványok kiválasztását. Például a 802.11n szabvány felülről kompatibilis a 802.11g és 802.11b szabványokkal, de a 802.11a-val nem. Ha a meglévő hálózati infrastruktúra és a használt berendezések a 802.11a szabványt támogatják, akkor az új megvalósításnak is támogatnia kell ezt a szabványt.

Az ár nem elhanyagolható tényező. Ha a költségeket vesszük figyelembe, számoljunk összköltséggel (TCO), mely magában foglalja a beszerzési és telepítési költségeket is. Egy közepes vagy nagyméretű vállalati környezetben az összköltségnek (TCO) sokkal nagyobb súlya van a választott WLAN szabványra nézve, mint az otthoni vagy kisvállalati környezetekben. Ez azért van, mert a nagyobb vállalatok esetében, több berendezésre és telepítési tervekre van szükség, melyek növelik a költségeket.

A vezeték nélküli eszközök telepítése

Az otthoni vagy kisvállalati környezetben, a telepítés általában csekély számú eszköz felszereléséből áll, melyek könnyen áthelyezhetőek az optimális lefedettség és áteresztőképesség eléréséhez.

A nagyvállalati környezetekben, a berendezéseket nem egyszerű áthelyezni és a lefedettségnek tökéletesnek kell lennie. Meg kell határozni a lefedettséghez szükséges hozzáférési pontok optimális számát és elhelyezését a lehető legalacsonyabb költség befektetésével.

Ezen célok eléréséhez, általában helyszíni felmérést (Site Survey) végeznek. A helyszíni felmérést végző személynek jól kell értenie a WLAN tervezéshez és számos bonyolult műszer segítségével meg kell tudnia állapítani a jelerősségeket és az interferencia mértékét. A telepítendő WLAN hálózat méretének függvényében ez nagyon költséges folyamat lehet. Kisebb méretű hálózatok esetén a helyszíni felmérést a vezeték nélküli állomással és a legtöbb vezeték nélküli hálózati csatolóhoz (NIC) adott segédprogram használatával végzik el.

Mindegyik esetben figyelembe kell venni az ismert zajforrásokat, például magas feszültségű vezetékeket, motorokat és egyéb vezeték nélküli berendezéseket, a WLAN eszközök helyének kiválasztásakor.

7.4.2 Egy AP telepítése és biztonsági beállításai

Miután meghatároztuk a legmegfelelőbb technológiát és az AP helyét, szereljük fel, és készítsük el a biztonsági beállításait. A biztonsági óvintézkedéseket még azelőtt meg kell tervezni és alkalmazni, mielőtt az AP-t az ISP-hez vagy a hálózathoz csatlakoztatnánk.

Néhány alapvető biztonsági intézkedés:

- A gyári értékek megváltoztatása az SSID, felhasználó nevek és jelszavak esetében.
- Az SSID szórásának letiltása
- MAC cím szűrés beállítása.

Néhány fejlett biztonsági intézkedés:

- WEP vagy WPA titkosítás használata
- Hitelesítés beállítása
- Forgalomszűrés alkalmazása

Tartsuk észben, hogy egyetlen biztonsági óvintézkedés önmagában nem képes teljesen megvédeni a hálózatot. Többféle technika együttes alkalmazása elősegíti a biztonsági terv integritását.

Amikor az állomások konfigurálására kerül sor, nagyon fontos, hogy az SSID-k megegyezzenek az AP-n beállított SSID-vel. Ezen kívül a titkosítási és hitelesítési kulcsoknak is meg kell egyezniük.

7.4.3 A konfigurációs állomyányok mentése és visszaállítása

Amikor a vezeték nélküli hálózat már megfelelően működik, érdemes az összes eszköz konfigurációs állományáról biztonsági mentést készíteni. Ez különösen akkor fontos, amikor testreszabott konfigurációkkal dolgozunk.

A legtöbb otthoni és kisvállalati felhasználásra forgalmazott integrált forgalomirányító esetén ez egyszerűen elvégezhető a megfelelő menü Backup Configurations (Konfiguráció biztonsági mentése) opciójának és az állomány mentési helyének kiválasztásával. Az integrált forgalomirányítók alapértelmezett néven mentik a konfigurációs állományt. Ennek az állománynak a nevét meg lehet változatni.

A visszaállítási folyamat is hasonlóan egyszerű. Válasszuk ki a Restore Configurations (konfiguráció visszaállítása) lehetőséget. Aztán, egyszerűen keressük az előzőleg mentett konfigurációs állományt.

Ha az állományt kiválasztottuk, kattintsunk a Start to Restore (visszaállítás megkezdése) gombra a feltöltés megkezdéséhez.

Némely esetben szükséges lehet a gyári alapértelmezett beállítások betöltése. Ennek eléréséhez vagy válaszzuk ki a megfelelő menü Restore Factory Defaults (Gyári beállítások visszaállítása) gombját vagy nyomjuk le és tartsuk lenyomva 30 másodpercig az eszköz RESET nyomógombját. Az utóbbi lehetőség különösen akkor hasznos, ha nem tudunk az integrált forgalomirányító hozzáférési pontjához hálózaton keresztül csatlakozni, de fizikailag hozzáférünk az eszközhöz.

7.4.4 A Frimware frissítése

A legtöbb intergrált forgalomirányító operációs rendszere firmware-ben van tárolva. Amikor új szolgáltatásokat fejlesztenek ki, vagy a meglévő firmware hibáit javítják ki, szükségessé válhat az eszköz firmware-jének frissítése.

Az integrált forgalomirányítók, mint amilyen a Linksys, firmware frissítési folyamata elég egyszerű. Fontos azonban tudnunk, hogy ha egyszer a folyamatot elkezdtük, nem szabad megszakítani. Ha a frissítési folyamat befejezés előtt megszakad, az eszköz működésképtelenné válhat.

Határozzuk meg az eszköz aktuálisan használt firmware verzióját. Ezt az információt általában a konfigurációs képernyőn vagy a kapcsolat állapota ablakban láthatjuk. Ezután, nézzünk utána a gyártó weboldalán és az ehhez kapcsolódó internetes híroldalakon, az újabb firmware szolgáltatások, a frissítéssel kapcsolatos garanciális problémák és a lehetséges frissítések meglétéről.

Töltse le az új firmware változatot, és mentse el egy az integrált forgalomirányítóval közvetlen kapcsolatban lévő számítógép merevlemezére. Előnyösebb, ha a számítógép kábel segítségével közvetlenül kapcsolódik a forgalomirányítóhoz. Ezzel megelőzhető, hogy a frissítési folyamat megszakadjon a vezeték nélküli kapcsolat bizonytalansága miatt.

Válassza ki a Firmware Upgrade lehetőséget a grafikus felületen (GUI)! Keresse meg a megfelelő állományt a közvetlenül kapcsolódó eszközön és indítsa el a frissítést!

7.5 A fejezet összefoglalása

A fejezet bemutatta a vezeték nélküli technológiák előnyeit és korlátait és e technológiákat használó készülékeket. A fejezet részletezte ezen technológiák és az azt használó berendezések előnyeit és korlátait.

- A vezeték nélküli technológiák az infomáció szállítására az eszközök között az elektromágneses sugárzást használják rádiójelek formájában.
- A leggyakoribb hulámhosszokat közhasznú vezeték nélküli kommunikációra használják, köztük az Infravörös és rádiófrekvenciás (Radio Frequency, RF) sávok bizonyos részét.
- A távvezérelhető eszközök, vezeték nélküli egerek és billentyűzetek az Infravörös (IR) vagy Bluetooth technológiák valamelyikét használják.
- Az olyan berendezések, mint mikrohullámú sütők vagy zsinórnélküli telefonok megzavarhatják a WLAN kommunikációt, mert hasonló frekvenciákon üzemelnek.
- A vezeték nélküli hálózatokat három nagy csoportra bonthatjuk: Vezeték nélküli személyi hálózatok (WPAN), Vezeték nélküli helyi hálózatok (WLAN), és Vezeték nélküli nagy kiterjedésű hálózatok (WWAN).
- A vezeték nélküli technikai szabványok létrehozásáért felelős elsődleges szervezet az IEEE. A WLAN környezetekben uralkodó szabványok: 802.11A, 802.11B, 802.11G és 802.11N, melyek Wi-Fi szabványokként is ismertek.

- A következő eszközöket tartalmazzák a WLAN-ok: vezeték nélküli ügyfelek, hozzáférési pontok (Access Point, AP), vezeték nélküli hidak és antennák.
- A kisebb WLAN-ok, melyek egyenrangú hálózatok, ad-hoc hálózatokként ismertek és nem tartalmaznak hozzáférési pontot.
- A vezeték nélküli eszközök antennákat használnak az információk vételéhez és adásához. Kétféle típusú antenna létezik: irányított és irányítattlan.
- Egy WLAN hálózatban lévő összes eszköz esetén ugyanazon SSID beállításokat kell elvégezni és azoknak egyazon szabvány szerint kell üzemelniük ahhoz, hogy kommunikálni tudjanak.
- Az egyes párbeszédek elkülönítéséhez, az RF tartományt különböző csatornákra osztották.
- A hozzáférési pontok és állomások az úgynevezett Vivőérzékeléses Többszörös Hozzáférésű Ütközéselkerüléses (CSMA/CA) közeghozzáférési technikát használják, mely lefoglalja a használandó csatornát az adott párbeszéd lebonyolításához.

Mivel a vezeték nélküli hálózatok képesek minimális beállítások mellett az adatok átvitelére a levegőn keresztül, a vezetékes hálózatokkal összevetve, jóval védtelenebbek a támadásokkal szemben.

- Egy támadó bárhonnan hozzáférhet a hálózatunkhoz ahova a vezetéknélküli jel elér.
- Ezzel a támadók ingyenesen vehetik igénybe az Internet elérésünket vagy kárt tehetnek az állományokban, illetve ellophatnak bizalmas információkat a hálózatról.
- A megteendő alapvető biztonsági óvintézkedések közé sorolhatók a következők:
  - A gyári értékek megváltoztatása az SSID, felhasználó nevek és jelszavak esetében.
  - Az SSID szórásának letiltása
  - MAC cím szűrés beállítása.
- A fejlettebb biztonsági intézkedések, melyeket egy vezeték nélküli biztonsági tervnek érdemes tartalmaznia:
  - WEP vagy WPA titkosítás használata
  - Hitelesítés beállítása
  - Forgalomszűrés alkalmazása

Egy vezeték nélküli hálózat telepítése előtt érdemes telepítési tervet készíteni, amely tartalmazza a használt szabványokat, az eszközök elhelyezését, a biztonsági tervet és a konfigurációs állományok mentésnek menetét.E terv megvalósításához a következő lépések szükségesek:

- **A felhasználói igények összegyűjtése** , amely a megfelelő szabvány kiválasztásához, a sávszélesség igény és a lefedettségi terület meghatározásához, a meglévő hálózati kiépítés megismeréséhez, illetve a költségek kiszámításához szükségesek.
- **Helyszíni felmérés (Site-Survey)** végzése a hozzáférési pontok optimális számának és helyének meghatározásához.
- **Többféle biztonsági technika** együttes alkalmazása a vezeték nélküli hálózat integritásának biztosításához.
- **A vezeték nélküli eszközök konfigurációinak mentése** , amely biztosítja a konfiguráció visszatöltését az eszközök meghibásodása esetén.
- **Az eszközök firmware-jének** frissítése, hogy igénybe lehessen venni az újabb szolgáltatásokat.

8. Hálózatbiztonsági alapok

8.1 A hálózati kommunikáció veszélyei

8.1.1 A hálózatba történő behatolás kockázati

A számítógép hálózatok - akár vezetékesek, akár vezeték nélküliek - egyre fokozódó mértékben válnak a mindennapos tevékenység elengedhetetlen részévé. A magánszemélyek és a szervezetek egyformán a számítógépeiktől és a hálózattól függenek olyan feladatokban, mint az elektronikus levelezés, a könyvelés illetve a szervezet és az állománykezelés. Egy jogosulatan személy behatolása költséges hálózati üzemszünetet és a munka elvesztését eredményezheti. A hálózat elleni támadás pusztító lehet és idő és pénzveszteséget eredményezhet a fontos információk vagy eszközök megrongálása vagy ellopása következtében.

A behatolók hozzáférést szerezhetnek a hálózathoz a szoftver sebezhető pontjain keresztül, hardver elleni támadással vagy akár kevésbé fejlett módszerekkel is, mint például a felhasználó nevének és jelszavának kitalálása. Azokat a behatolókat, akik szoftver módosításával vagy a szoftver sebezhető pontjait kihasználva jutnak hálózati hozzáféréshez gyakran hekkereknek (hacker) nevezzük.

Ha egyszer a hekker hálózati hozzáféréshez jut, akkor a veszély négy típusa merülhet fel:

- Információlopás
- Azonosító ellopása
- Adatvesztés illetve manipulálás
- Szolgáltatás megszakítása

Információlopás

Betörés egy számítógépbe bizalmas információk megszeruése céljából. Az információ felhasználható vagy értékesíthető különböző célokra. Pédául: egy szervezet tulajdonát képező olyan információ eltulajdonítása, mint a kutatási és fejlesztési információk.

Adatvesztés és manipuláció

Betörés egy számítógépbe adatrekordok megszeruése vagy módosítása céljából. Példa az adatlopásra: vírus küldése, mely megformázza a számítógép merevlemezét. Példa az adatmanipulációra: betörés egy nyilvántartó rendszerbe olyan információ megváltoztatása céljából, mint egy tétel egységára.

Azonosító ellopása

Az információlopás egy formája ahol a személyes információt tulajdonítják el valaki azonosságának átvétele céljából. Ezt az információt felhasználva egy személy hozzájuthat hivatalos dokumentumokhoz, hitelt igényelhet és jogosulatlan Internetes vásárlásokat végezhet. Az azonosító ellopása egyre növekvő probléma, mely évente több milliárd dollár költséget okoz.

Szolgáltatás megszakítása

A hivatalos felhasználók megakadáyozása abban, hogy hozzáférjenek azokhoz a szolgáltatásokhoz, melyre jogosultak.

8.1.2 A hálózati behatolás forrásai

A hálózatba behatolóktól eredő biztonsági veszélyek mind belső, mind külső forrásból származhatnak.

Külső veszélyek

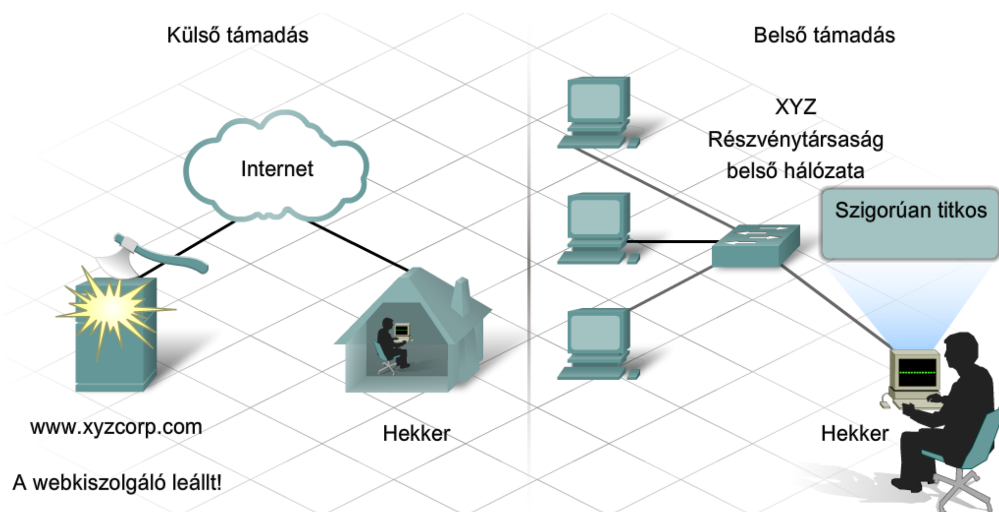
A külső veszélyek a szervezeten kívül dolgozó személyekkel kapcsolatban merülnek fel. Ők nem rendelkeznek hozzáférési jogosultsággal a számítógép rendszerekhez vagy hálózathoz. A külső támadók a hálózatba való bejutásukat főleg az Interneten, vezeték nélküli kapcsolatokon vagy a szerverekhez történő behívásos hozzáférésen keresztül hajtják végre.

Belső veszélyek

A belső veszélyek akkor jelentkeznek, amikor valaki egy felhasználói fiókon keresztül hozzáférési jogosultsággal rendelkezik a hálózathoz, vagy fizikailag hozzáfér a hálózati eszközhöz. A belső támadó ismeri a belső szabályokat és embereket. Gyakran azt is tudja, melyik információk értékesek és egyben sebezhetők és, hogy miként lehet ezeket elérni.

Azonban nem minden belső támadás szándékos. Sok esetben a belső veszély egy olyan megbízható alkalmazottól eredhet, aki vírust vagy biztonsági veszélyt szed össze míg a vállalaton kívül tartózkodik és akaratlanul behozza ezeket a belső hálózatba.

Legtöbb vállalat tekintélyes összegeket költ a külső támadások elleni védekezésre, miközben a legtöbb veszély belső forrásból származik. Az FBI szerint a belső hozzáférések és a számítógépes rendszerekkel történő visszaélések az összes jelentett biztonsági behatolási eseménynek megközelítőleg a 70%-át teszik ki.



8.1.3 Megtévesztési technika (Social Engineering) és adathalászat

Egy behatoló számára a hozzáféréshez jutás egyik legegyszerűbb módja akár belülről akár kívülről, az emberi hiszékenység kihasználása. Az emberi gyengeség kihasználásának egyik gyakoribb módszerét megtévesztési technikának (Social Engineering, 'A megtévesztés művészete', K. Mitnick,2003) nevezzük.

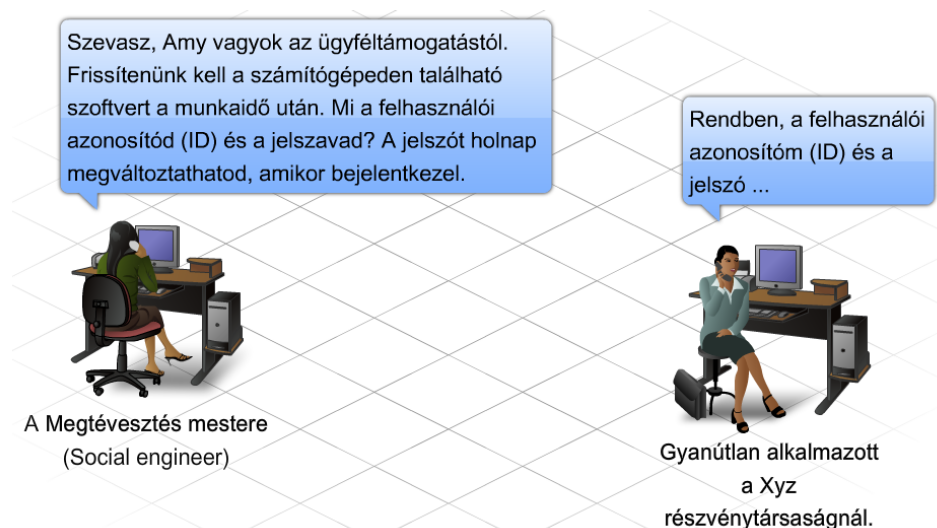
Megtévesztési technika (Social Engineering)

A megtévesztési technika valaki vagy valami azon képességére utaló kifejezés, mellyel befolyásolja egy embercsoport viselkedést. Számítógép és hálózatbiztonsági szövegkörnyezetben a megtévesztési technika a technikák egy olyan csoportjára vonatkozik, mellyel ráveszik a belső felhasználókat arra, hogy adott tevékenységet végrehajtsanak vagy titkos információkat kiszolgáltassanak.

Ezekkel a technikákkal a támadók félrevezetik a gyanútlan, jogosult felhasználókat azért hogy hozzáférjenek a belső erőforrásokhoz, és olyan személyes információkhoz, mint a bankszámlaszámok vagy jelszavak.

A megtévesztési technika típusú támadások azt a tényt használják ki, hogy a biztonság leggyengébb láncszemének általában a felhasználót tekintjük. A megtévesztés mesterei (Social engineers) lehetnek a szervezeten belül vagy kívül, azonban leggyakrabban nem álllnak ki nyíltan az áldozatuk elé.

A három legáltalánosabban használt megtévesztési technika (social engineering): a hamis ürügy (pretext), az adathalászat (phishing) és a telefonos adathalászat (vishing).



Hamis ürügy (Pretexting).

A hamis ürügy (Pretexting) a megtévesztési technika egyik olyan formája, ahol egy előre megtervezett esetet (pretext) használnak fel az áldozat megtévesztésére azért, hogy információkat adjon vagy végrehajtson egy tevékenységet. A célszeméllyel jellegzetesen telefonon keresztül lépnek kapcsolatba. Ahhoz hogy a hamis ürügy hatékony legyen a támadónak képesnek kell lennie arra, hogy megalapozza a hitelét a célszemély, illetve az áldozat előtt. Ez a támadó részéről gyakran előzetes tanulmányozást vagy kutatást követel meg. Például ha a támadó ismeri a célszemély társadalombiztosítási számát, ezt az információt felhasználhatja arra, hogy elnyerje a célszemély bizalmát. Ekkor a célszemély nagyobb valószínűséggel ad meg további információkat.

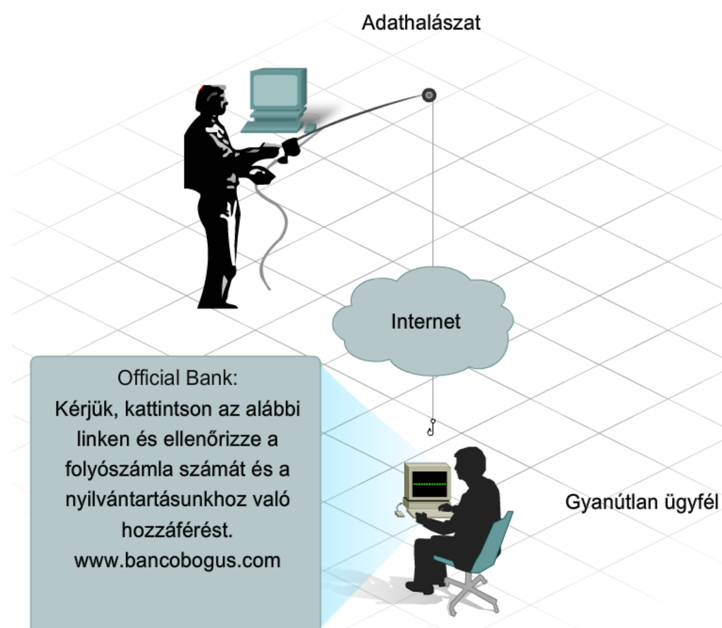
Adathalászat (Phishing)

Az adathalászat a megtévesztési technika olyan formája, ahol az adathalászok úgy tesznek mintha egy a szervezeten kívüli hivatalt képviselnének. Tipikusan elektronikus levélen keresztül személyesen

lépnek kapcsolatba a célszeméllyel (a 'hallal'). Az adathalász olyan hitelesítési információkat kérhet, mint a jelszó vagy a felhasználói név azért, hogy valami szörnyű következmények bekövetkezésétől óvjon meg.

Telefonos adathalászat (Vishing/Phone Phishing)

A megtévesztési technika azon új formája, ahol az IP-n keresztüli hangtovábbítást (VoIP) használják, telefonos adathalászatként (vishing) ismert. A telefonos adathalászatnál a gyanútlan felhasználóknak levelet küldenek, melyben utasítják őket, hogy hívják fel azt a számot, mely egy hivatalos telebank szolgáltatás számának néz ki. A hívást a tolvaj kapja meg. A telefonon keresztül, hitelesítés céljából megadott bankszámlaszámot vagy jelszót így ellopják.



8.2 Támadás módszerek

8.2.1 Vírusok, férgek és Trójai lovak

A megtévesztési technika egy általános biztonsági veszély, mely az emberi gyengeséget ragadja meg ahhoz, hogy elérje a kívánt eredményt.

A megtévesztési technikán kívül vannak más olyan támadástípusok is, melyek a számítógépes szoftverek sebezhető pontjait használják ki. E támadási technikák közé tartoznak: a vírusok, férgek és Trójai lovak. Ezeknek a rosszindulatú szoftvereknek mindegyike egy állomáson telepszik meg. Károsíthatják a rendszert, megsemmisíthetik az adatokat illetve megtilthatják a hozzáférést a hálózatokhoz, rendszerekhez vagy szolgáltatásokhoz. Ezenkívül adatokat és személyes információkat továbbíthatnak a gyanútlan PC felhasználóról a támadónak. Sok esetben sokszorosítják és terjesztik magukat a hálózat más állomásaira is.

Időnként ezeket a technikákat a megtévesztési technikákkal együtt használják, hogy ravaszul rávegyék a gyanútlan felhasználót a támadás végrehajtására.

Vírusok

A vírus egy program, mely lefut és más programok vagy fájlok módosításával terjed. A vírus önmagát nem tudja futtatni, szüksége van arra, hogy aktíválják. Ha egyszer aktíválva lett, a vírus nem képes mást tenni, mint sokszorosítja magát és továbbterjed. Egyszerűsége ellenére ez a fajta vírus veszélyes, mivel gyorsan felemészti az összes rendelkezésre álló memóriát és a rendszer leállását idézheti elő. A még veszélyesebb vírust úgy is programozhatják, hogy meghatározott állományokat töröljön vagy megfertőzzön, mielőtt továbbterjed. A vírusok továbíthatók e-mail mellékletként, letölttött állományokkal, azonnali üzenetekkel vagy lemezen, CD-n vagy USB eszközön keresztül.

Férgek

A féreg hasonló a vírushoz, de a vírustól eltérően nincs szüksége arra, hogy egy programhoz kapcsolódjon. A féreg a hálózatot használja arra, hogy elküldje saját másolatát bármelyik kapcsolódó állomásra. A férgek önállóan tudnak futni és gyorsan terjednek. Nem igényelnek szükségszerűen aktíválást vagy emberi közbeavatkozást. A saját-terjesztésű hálózati férgek jóval nagyobb hatással lehetnek, mint egy egyedi vírus és az Internet nagy részeit gyorsan megfertőzhetik.

Trójai lovak

A Trójai ló egy önmagát nem sokszorosító program, mely úgy készült, hogy hivatalos programként jelenjen meg, miközben valójában egy támadási eszköz. A Trójai ló a hivatalos megjelenésére alapozva veszi rá az áldozatot arra, hogy indítsa el a programot. Viszonylag ártalmatlan lehet, de olyan kódot is tartalmazhat, mely károsíthatja a számítógép merevlemezének tartalmát. Ezen kívül a Trójai vírusok egy hátsó kaput (back door) is létesíthetnek a rendszeren, mely a hekkerek hozzéféréshez jutását teszi lehetővé.

8.2.2 Szolgáltatás-megtagadás (DoS) és Nyers erő (Brute Force) típusú támadások

Időnként egy támadó célja az, hogy megakadályozza a hálózat normál működését. Az ilyen típusú támadásokat rendszerint azzal a szándékkal hajtják végre, hogy összeomlasszák egy szervezet működését.

Szolgáltatás-megtagadás (Denial of Service, DoS)

A DoS támadások személyi számítógépek vagy számítógépek egy csoportja elleni agresszív támadások, melyeknek az a célja, hogy meggátolja a potenciális felhasználókat a szolgáltatások igénybe vételében. A DoS támadások irányulhatnak végfelhasználói rendszerek, kiszolgálók és hálózati összeköttetések ellen is.

Általában a DoS támadások a következőket kísérlik meg:

Forgalommal árasztják el a rendszert vagy a hálózatot, hogy megakadályozzák a hivatalos hálózati forgalom működését.

Megszakítják az ügyfél és a kiszolgáló közötti kapcsolatokat, hogy megakadályozzák a szolgáltatáshoz való hozzáférést.



A DoS támadásnak számos típusa van. A biztonságért felelős rendszergazdáknak tájékozottnak kell lenniük azokról a DoS támadástípusokról melyek előfordulhatnak és meg kell győződniük arról, hogy a hálózataik védve vannak. A gyakori DoS támadások:

SYN (szinkron) elárasztás - egy csomagáradat kerül elküldésre a kiszolgálóhoz kérve az ügyfél kapcsolódását. A csomagok érvénytelen forrás IP-címet tartalmaznak. A kiszolgálót teljesen lefoglalja az, hogy megpróbálja megválaszolni ezeket a hamis kéréseket és így nem képes válaszolni a valódiakra.

Halálos ping: egy olyan csomag kerül elküldésre az eszköznek, melynek mérete meghaladja az IP által megengedett méretet (65.535 bájt). Ez a fogadó rendszer összeomlását okozza.

Elosztott szolgáltatás-megtagadás (Distributed Denial of Service, DDoS)

A DDoS egy kifinomultabb és kártékonyabb formája a DoS támdásnak. Úgy tervezték, hogy haszontalan adatokkal árassza el és telítse a hálózati összeköttetéseket. A DDoS jóval nagyobb léptékben működik, mint a DoS. Tipikusan támadási pontok százai és ezrei kísérelnek meg elárasztani egyidejűleg egyetlen célt. A támadási pontok olyan gyanútlan számítógépek lehetnek, melyek megelőzően már megfertőződtek a DDoS kóddal. A DDoS kóddal fertőzött rendszerek támadást intéznek a célhely ellen, amikor meghívják őket.

Nyers erő (Brute force)

Nem minden támadás kifejezetten DoS támadás, mely a hálózat leállását okozza. A nyers erő (Brute Force) módszerét alkalmazó támadás egy másik típusa azoknak a támadásoknak, melyek szolgáltatás-megtagadást eredményezhetnek.

A nyers erőt alkalmazó támadásnál egy gyors számítógép használatával kísérlik meg kitalálni a jelszavakat vagy visszafejteni egy titkosítási kódot. A támadó gyors egymásutánban kellően nagyszámú lehetőséget próbál ki ahhoz, hogy hozzáféréshez jusson vagy feltörje a kódot. A nyers erő (brute force) módszerét alkalmazó támadások szolgáltatás-megtagadást okozhatnak a rendkívül magas forgalom következtében egy meghatározott erőforrásnál vagy a felhasználói fiók zárolásával.

8.2.3 Kémprogramok, nyomkövető sütik, reklámprogramok és előugró ablakok

Nem minden támadás okoz károkat vagy akadályozza meg a hivatalos felhasználót abban, hogy hozzáférjen az erőforrásokhoz. Számos veszélyforrást úgy terveztek, hogy hirdetési, piacszervezési és kutatási célokra felhasználható információt gyűjtsön a felhasználókról. Ezek közé tartoznak a kémprogramok (spyware), a nyomkövető sütik (tracking cookie) és előugró ablakok (pop-up). Miközben ezek nem károsíthatják a számítógépet, betörnek a magánszférába és bosszantóak lehetnek.

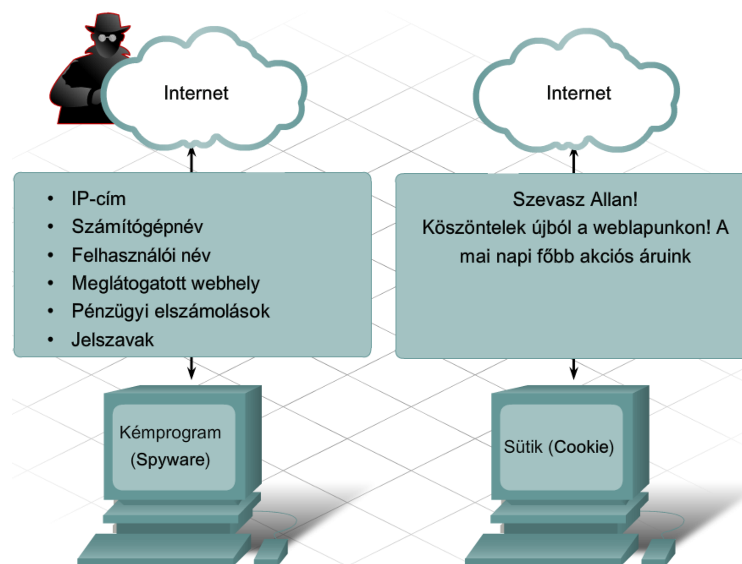
Kémprogram (spyware)

Bármely olyan program kémprogram, mely személyes információt gyűjt a számítógépről a hozzájárulásunk vagy tudomásunk nélkül. Ez az információ az Internetes reklámozókhoz vagy másokhoz kerül megküldésre és jelszavakat és számlaszámokat tartalmazhat.

A kémprogram telepítése rendszerint tudtunkon kívül történik, amikor letöltünk egy állományt, másik programot telepítünk vagy egy előugró ablakon (pop-up) kattintunk. Lelassíthatják a számítógépet és megváltoztathatják a belső beálításokat további sebezhető pontokat létrehozva más támadások számára. Ráadásul a kémprogramot (spyware) nagyon nehezen lehet eltávolítani.

Nyomkövető sütik (tracking cookie)

A süti (cookie) a kémprogram egy formája, de nem mindig rossz-szándékú. Az Internetet használókról szokott információt rögzíteni, mikor azok meglátogatják a wehelyeket. A sütik (cookie) a megszemélyesítés engedélyezésével illetve időmegtakarítási technikák következtében hasznosak vagy kívánatosak is lehetnek. Sok webhely elvárja, hogy a sütik (cookie) engedélyezve legyenek a felhasználó kapcsolódásának engedélyezéséhez.



Reklámprogram (adware)

A reklámprogram (adware) a kémprogram egy olyan formája, melyet egy felhasználóról történő információgyűjtésre használnak azokra a webhelyekre alapozva, melyeket a felhasználó meglátogat. Ezeket az információkat azután célzott hirdetésekre használják. A reklámprogramot általában a felhasználó telepíti egy "ingyenes" termékért cserében. Amikor a felhasználó megnyit egy böngészőablakot, a reklámprogram egy új böngészőpéldányt indíthat, melyen keresztül megpróbál a felhasználó szörfözési gyakorlatán alapuló termékeket vagy szolgáltatásokat reklámozni. A nem kívánatos böngészőablak újra és újra megnyílhat és nagyon megnehezítheti az Interneten való szörfözést, különösen lassú Internet kapcsolat mellett. A reklámprogramot (adware) nagyon nehezen lehet eltávolítani.

Előugró és mögényíló ablakok (pop-up és pop-under)

Az előugró (pop-up) és mögé nyíló (pop-under) ablakok olyan újabb ablakok, melyek akkor jelennek meg, amikor meglátogatunk egy webhelyet. A reklámprogramtól eltérően az előugró (pop-up) és mögé nyíló (pop-under) ablakoknak nem céljuk az információgyűjtés a felhasználóról, és jellegzetesen csak a meglátogatott webhelyhez társulnak.

- Előugró ablakok (pop-up): az aktuális böngészőablak előtt nyílnak meg.

- Mögényíló ablakok (pop-under): az aktuális böngészőablak mögött nyílnak meg.

Bosszantóak lehetnek és rendszerint nemkívánatos termékeket és szolgáltatásokat reklámoznak.

8.2.4 Levélszemét (spam)

Az elektronikus kommunikációba vetett fokozódó bizalmunk egyik bosszantó melléktermékе a tömeges nemkívánatos elektronikus levél. Időnként a kereskedők nem akarnak célzott értékesítéssel zavarni. E-mail hirdetéseiket akarják eljuttatni a lehető legtöbb felhasználónak azt remélve, hogy valaki érdeklődik a termékük vagy szolgáltatásuk iránt. A termékértékesítésnek ezen a széleskörű terjesztésen alapuló megközelítését az Interneten levélszemétnek (spam) hívják.

A levélszemét egy súlyos hálózati veszély, mely túlterhelheti az internetszolgáltatókat (ISP), levelezőkiszolgálókat és az egyéni végfelhasználói rendszereket. A levélszemét (spam) küldéséért felelős személyt vagy szervezetet szemetelőnek (spammer) nevezzük. A szemetelők (spammer) gyakran a nem biztonságos levelezőszervereket használják fel az elektronikus levél továbbítására. A szemetelők (spammer) olyan hekkelési technikákat használhatnak, mint a vírusok, férgek és Trójai lovak ahhoz, hogy átvegyék az otthoni számítógépek feletti ellenőrzést. Ezt követően ezeket a számítógépeket használják a levélszemét küldésére a tulajdonos tudta nélkül. A levélszemét elküldhető elektronikus levéllel vagy újabban azonnali üzenetküldő szoftveren keresztül is.

Úgy becsülik, hogy minden Internetes felhasználó évente több mint 3000 elektronikus levélszemetet kap. A levélszemét nagy Internet sávszélességet emészt fel és eléggé súlyos probléma ahhoz, hogy sok ország jelenleg már rendelkezik a levélszemét használatát szabályzó törvénnyel.

8.3 Biztonságpolitika

8.3.1 Általános biztonsági intézkedések

A biztonsági kockázatok nem küszöbölhetők ki vagy nem védhetők ki teljes mértékben. Azonban a hatékony kockázatkezelés és értékelés jelentősen minimalizálhatja a meglevő biztonsági kockázatokat. A kockázat mértékének minimalizálása céljából fontos megérteni azt, hogy egyedül egy termék nem tehet egy szervezetet biztonságossá. Valódi hálózati biztonság a termékek és szolgáltatások kombinációját egyesítő átfogó biztonságpolitikából és a politkához való ragaszkodásra való elkötelezettségből származik.

A biztonságpolitika a szabályok egy olyan hivatalos kinyilatkoztatása, amelyhez a felhasználóknak tartaniuk kell magukat, amikor fontos információhoz és technológiához férnek hozzá. Ez lehet egy egyszerű házirend, de lehet sok száz oldal terjedelmű is, amely részletezi a felhasználói kapcsolatok és hálózathasználati eljárások minden szempontját. A biztonságpolitikának kell állnia a hálózati biztonság meghatározásának, megfigyelésének, tesztelésének és továbbfejlesztésének a középpontjában. Míg a legtöbb otthoni felhasználó nem rendelkezik hivatalos írott biztonságpolitikával, ahogy a hálózat mérete és hatóköre nő, úgy nő a fontossága egy minden felhasználóra vonatkozó egyértelműen meghatározott biztonságpolitikának. Néhány terület, melyet a biztonságpolitikának tartalmaznia kell: azonosítási és hitelesítési házirend, jelszó házirend, elfogadható használatra vonatkozó házirend, távoli hozzáférés házirendje és váratlan események kezelésének eljárásai.

Ahhoz, hogy a biztonságpolitikában leírtak hatásosak legyenek, hálózat minden felhasználójának támogatnia kell és be kell tartania a biztonságpolitika előírásait.

Azonosítási és hitelesítési politika

- Meghatározza azokat a feljogosított személyeket, akik hozzáféréssel rendelkezhetnek a hálózati erőforrásokhoz valamint a hitelesítési eljárásokat.
- Ehhez hozzá tartozik a fizikai hozzáférés a huzalozási központokhoz és olyan kritikus hálózati erőforrásokhoz is mint a szerverek, kapcsolók, forgalomirányítók vagy hozzáférési pontok.

Jelszóházirendek

- Gondoskodik arról, hogy a jelszavak feleljenek meg a minimumkövetelményeknek és rendszeresen módosításra kerüljenek.

Elfogadható használat rendje

- Azonosítja az elfogadható hálózati alkalmazásokat és használatokat.

Távoli hozzáférés rendje

- Azonosítja, hogy hogyan férhetnek a távoli felhasználók hozzá egy hálózathoz és mi az ami elérhető távoli kapcsolaton keresztül.

Hálózat karbantartási eljárás

- Meghatározza a hálózati eszköz operációs rendszerek, és végfelhasználói alkalmazások frissítési eljárásait.

Váratlan esemény kezelésének eljárásai

- Leírja, hogy hogyan kell kezelni a biztonsági eseményeket.

A biztonságpolitikának kell állnia a hálózati biztonság meghatározásának, megfigyelésének, tesztelésének és továbbfejlesztésének a középpontjában. A biztonságpolitikákat biztonsági eljárások valósítják meg. Az eljárások az állomások és hálózati eszközök konfigurálásának, bejelentkezési módszereinek, ellenőrzésének és karbantartásának folyamatát határozzák meg. Tartalmazzák a kockázat csökkentése érdekében megteendő óvintézkedéseket csakúgy, mint a megismert biztonsági veszélyek elhárításának módszereit. A biztonsági eljárások kiterjednek az olyan egyszerű és olcsó megoldásokra, mint a szoftververziók naprakész állapotban tartása, az olyan összetett megvalósításokig, mint a tűzfalak és behatolás érzékelő rendszerek.

A hálózati biztonság megvalósításában használt néhány alkalmazás és biztonsági eszköz:

- Szoftver kiegészítések és frissítések
- Vírusvédelem
- Kémprogramok elleni védelem
- Levélszemét szűrők
- Előugró ablak blokkolók
- Tűzfalak

Tűzfal
Egy biztonsági eszköz, mely a hálózatba befelé vagy onnan kifelé irányuló forgalmat ellenőrzi.

Levélszemét szűrő
Egy végfelhasználói munkaállomáson vagy kiszolgálón telepített szoftver a nemkívánatos elektronikus levelek azonosítására és eltávolítására.

Kiegészítések és frissítések
Egy OS vagy alkalmazás számára felhasznált szoftver egy ismert biztonsági hiányosság kiküszöbölésére vagy újabb feladatok ellátására.

Kémprogram-irtó
Egy végfelhasználói munkaállomáson telepített szoftver a kémprogramok és reklámprogramok észlelésére és eltávolítására.

Előugró ablak blokkoló
Egy végfelhasználói munkaállomáson telepített szoftver az előugró és mögényíló hirdetési ablakok megjelenésének kiküszöbölésére.

Vírusirtó
Egy végfelhasználói munkaállomáson vagy kiszolgálón telepített szoftver a vírusok, férgek és Trójai lovak észlelésére és az állományokból illetve elektronikus levélből történő eltávolítására.

8.3.2 Frissítések és kiegészítések (patch)

A hekker (hacker) leggyakrabban a szoftverek sebezhető pontjait használják ki az állomásokhoz vagy hálózatokhoz való hozzáféréshez. Fontos, hogy a szoftveralkalmazásokat a legutolsó kiegészítő csomagokkal (patch) és frissítésekkel naprakész állapotban tartsuk a veszélyek elhárítására. A kiegészítés (patch) egy kis kódrészlet, amely egy meghatározott problémát orvosol. A frissítés pedig új szolgáltatásokkal egészíti ki a teljes szoftvercsomagot amellett, hogy a meghatározott problémák javítását is elvégzi.

Az OS (operációs rendszer, pl. Linux, Windows, stb.) és alkalmazásgyártók folyamatosan kiadják a szoftver ismert sebezhető pontjait kijavító frissítéseket és biztonsági kiegészítéseket. Ezen kívül a gyártók gyakran bocsátanak ki frissítések és kiegészítők gyűjteményéből álló szervizcsomagokat is. Szerencsére sok operációs rendszer az automatikus frissítés lehetőségét is biztosítja, amely automatikusan letölti és telepíti az OS és az alkalmazások frissítéseit az állomásokon.

8.3.3 Vírusirtó szoftver

Még ha az OS és az alkalmazások rendelkeznek is az összes és legújabb kiegészítéssel, frissítéssel, akkor is támadások áldozatává válhatnak. Bármely eszköz, mely a hálózathoz kapcsolódik ki van téve a vírusoknak, férgeknek és Trójai lovaknak. Ezek felhasználhatók az OS kód megfertőzésére, a számítógép teljesítményének befolyásolására, alkalmazások megváltoztatására és adatok megsemmisítésére.

Vírus, féreg vagy Trójai ló jelenlétére utaló jelek:

- A számítógép rendellenesen kezd működni.
- Egy program nem érzékeli az egeret vagy a billentyűzetet.
- Egy program saját magától elkezd futni vagy leáll.
- Az e-mail program nagy mennyiségű elektronikus levelet kezd el küldeni.
- A CPU kihasználtsága nagyon nagy.
- Nem azonosítható vagy nagyszámú folyamat fut.
- A számítógép jelentős mértékben lelassul, vagy a rendszer összeomlik.

A vírusirtó szoftver megelőző eszközként és aktív, reagáló eszközként egyaránt használható. Megakadályozza a fertőzést, észleli és eltávolítja a vírusokat, férgeket és Trójai lovakat. A vírusirtó szoftvert minden olyan számítógépre telepíteni kell, amelyik a hálózatra kapcsolódik. Számos vírusirtó szoftver áll rendelkezésre.

Néhány olyan tulajdonság, mellyel a vírusirtó programok rendelkeznek az alábbi:

- **Elektronikus levél ellenőrzése** - átvizsgálja a bejövő és kimenő leveleket és azonosítja a gyanús mellékleteket.
- **Memóriarezidens dinamikus vizsgálat** - ellenőrzi a végrehajtható fájlokat és dokumentumokat, amikor azokhoz hozzáférnek.
- **Ütemezett vizsgálat** - a víruskeresést ütemezni lehet, hogy szabályos időközönként lefusson és ellenőrizze a kiválasztott meghajtókat vagy az egész számítógépet.
- **Automatikus frissítés** - utánanéz és letölti az ismert vírusjellemzőket és mintákat. Ütemezni lehet, hogy a frissítéseket szabályos időközönként ellenőrizze le.

A vírusirtó szoftver az eltávolítandó vírus ismeretére támaszkodik. Ezért fontos, hogy a vírus azonosításáról vagy bármely más vírusra utaló tevékenységről beszámoljunk a hálózati rendszergazdának. Ez rendszerint egy esetbeszámoló benyújtásával történik a vállalat hálózati biztonságpolitikájával összhangban.

A hálózati rendszergazdák a fenyegetési eseményekről beszámolhatnak a helyi hivatalos ügynökségnek is, amely a biztonsági problémákat kezeli. Például ilyen ügynökség az USA-ban:https://forms.us-cert.gov/report/ Ez az ügynökségfelelős az új vírusfenyegetések elleni intézkedések kidolgozásáért valamint gondoskodni arról, hogy ezek az intézkedések a legkülönbözőbb vírusirtó szoftverfejlesztők számára is rendelkezésre álljanak .

8.3.4 Levélszemét irtó (anti-spam)

A levélszemét (spam) nem csupán bosszantó jelenség. Túlterheti a levelező-kiszolgálókat és potenciálisan vírust és más biztonsági veszélyt is hordozhat. Ezenkívül a szemetelők (spammer) vírust vagy Trójai programot tartalmazó kód telepítésével átveszik az ellenőrzést az állomás fölött. Ezt követően az állomást a felhasználó tudta nélkül levélszemetet tartalmazó elektronikus levelek küldésére használják. Az ilyen módon fertőzött számítógép levélszemét üzem (spam mill) néven ismert.

A levélszemét-irtó szoftver azonosítja a levélszemetet, majd szeméttároló mappába (karanténba) helyezi vagy törli. A levélszemét irtó szoftver futhat a munkaállomáson vagy a levelezőkiszolgálón is. Ezen kívül sok ISP végez levélszemét-szűrést is. A levélszemét-irtó szoftver nem ismer fel minden levélszemetet, így fontos, hogy óvatosan nyissunk meg leveleinket. Néha a hasznos leveleinket is véletlenül levélszemétként azonosítja és kezeli.

A levélszemét-blokkolók használatán kívül a levélszemét terjedésének megelőzésére az alábbi óvintézkedéseket érdemes megtennie:

- Rendszeresen telepítése az operációs rendszer és az alkalmazások frissítéseit.
- Rendszeresen futtassa, és tartsa naprakész állapotban a vírusirtó programját.
- Ne továbbítson gyanús elektronikus leveleket.



- Ne nyisson meg levélmellékleteket, különösen azokat ne, amelyek ismeretlen személytől származnak.
- Készítsen üzenetszabályokat a levelezőprogramban azoknak a levélszemeteknek (spam) a törlésére, amelyek megkerülték a levélszemét-irtó szoftvert.
- Azonosítsa a levélszemét forrását és tájékoztassa erről a hálózati rendszergazdát, hogy az e forrásokból származó leveleket a továbbiakban szűrje ki.
- Számoljon be az esetről annak a hivatalos ügynökségnek, mely a levélszeméttel történő visszaélésekkel foglalkozik.

A levélszemét egy igen gyakori típusa a vírusfigyelmeztetés. Míg némely eletronikus levélben küldött vírusfigyelmeztetés valódi, addig nagy számuk ún. hoax, amely valójában nem létezik. Az ilyen típusú levélszemét problémát okozhat, mivel az emberek másokat is figyelmeztetnek a fenyegető katasztrófahelyzetre, és így ez elárasztja a levelezőrendszert. Ezen kívül a hálózati rendszergazdák is túlreagálhatják az esetet, és időt vesztegetnek olyan probléma felderítésére, amely nem is létezik. Végül, az ilyen elektronikus levelek hozzájárulhatnak a vírusok, férgek és Trójai lovak terjedéséhez. A vírusfigyelmeztető levél továbbítása előtt egy megbízható forrás segítségével: (pl.: http://vil.mcafee.com/hoax.asp, http://hoaxbusters.ciac.org/) ellenőrizze, hogy nem hoax-ról van-e szó.

8.3.5 Kémprogramirtó

Kémprogram- és Reklámprogram irtó

A kémprogram (spyware) és reklámprogram (adware) is vírusjellegű tüneteket okozhat. A jogosulatlan információgyűjtésen kívül jelentős számítógép erőforrásokat foglalhatnak le és befolyásolják a teljesítményt. A kémprogramirtó szoftver észleli és törli a kémprogram alkalmazásokat, valamint meggátolja a jövőbeni telepítésüket. Számos kémprogramirtó alkalmazás tartalmazza a sütik (cookie) és reklámprogramok (adware) észlelésének és törlésének lehetőségét is. Néhány vírusirtó csomag rendelkezik kémprogramirtó funkcióval is.

Előugró ablak (pop-up) blokkolók

Az előugró ablak blokkoló egy telepíthető szoftver az előugró (pop-up) és mögényíló (pop-under) ablakok elleni védekezésre. Számos webböngészőbe már beépítették az előugró ablak blokkoló szolgáltatást. Megjegyezzük, hogy néhány program és weboldal esetében ténylegesen szükség van az előugró ablakok megnyitására. A legtöbb előugró ablak blokkoló e célból felülbírálási lehetőséget biztosít.

8.4 Tűzfalak használata

8.4.1 Mi a tűzfal?

A hálózatra kapcsolt személyi számítógépek és kiszolgálók védelmén kívül fontos a hálózatba érkező és onnan kimenő forgalom ellenőrzése is.

A tűzfal az egyik leghatékonyabb olyan biztonsági eszköz, mely a belső hálózati felhasználók külső veszélyektől való megvédésére rendelkezésre áll. A tűzfal két vagy több hálózat között helyezkedik el és ellenőrzi a közöttük zajló forgalmat, valamint segíti a jogosulatlan hozzáférés elleni védelmet. A

tűzfal termékek változatos technikákat használnak annak meghatározására, hogy mely forgalom számára legyen engedélyezve vagy tiltva a hálózathoz való hozzáférés.

- **Csomagszűrés** - az IP vagy MAC-cím alapján akadályozza meg vagy engedélyezi a hozzáférést.
- **Alkalmazás/Webhely szűrés** - Az alkalmazás alapján akadályozza meg vagy engedélyezi a hozzáférést. A webhelyek, egy meghatározott weblap URL címe vagy kulcsszavak alapján blokkolhatók.
- **Állapot-alapú csomagvizsgálat (Stateful Packet Inspection, SPI)** - A bejövő csomagok csak a belső hálózat állomásairól kezdeményezett kérések válaszcsomagjai lehetnek. A nem kívánatos csomagokat külön engedély hiányában kiszűri. Az SPI felismerhet és kiszűrhet bizonyos típusú támadásokat is (pl.: DoS).

A tűzfal-termékek akár többféle szűrést is támogathatnak. Ezen kívül a tűzfalak gyakran hálózati címfordítást (Network Address Translation, NAT) is végeznek. A NAT egy belső címet, vagy címek csoportját egy olyan külső, nyilvános címre fordítja, mely a hálózaton keresztül továbbítva lesz. Ez lehetővé teszi a belső címek külső felhasználók elől való elrejtését.

A tűzfal termékek számos különböző formában készülnek:

- **Eszköz-alapú tűzfal** - az eszköz-alapú tűzfal egy biztonsági készülékként ismert célhardverbe van beépítve.
- **Kiszolgáló-alapú tűzfal** - a kiszolgáló-alapú tűzfal egy tűzfalalkalmazás, amely valamilyen hálózati operációs rendszer alatt fut (Network OS: UNIX, Windows, Novell).
- **Integrált tűzfal** - az integrált tűzfal egy meglevő eszköz (pl.: forgalomirányító) tűzfalszolgáltatással kiegészítve.
- **Személyes tűzfal** - a személyes tűzfal a munkaállomáson helyezkedik el, nem LAN megvalósításra tervezték. Lehet az operációs rendszer beépített szolgáltatása, vagy származhat külső gyártótól is.

Cisco biztonsági berendezések

Tűzfal céleszköz egyedi számítógépekkel, melyek nem rendelkeznek perifériával és merevlemezzel. Az eszköz-alapú tűzfal gyorsabban képes a forgalmat megvizsgálni és kevésbé hajlamos a meghibásodásra.

Kiszolgáló-alapú tűzfal

Tűzfal alkalmazások, melyek általában olyan megoldást biztosítanak, mely egy SPI tűzfalat és az IP-cím vagy alkalmazás alapú hozzáférésvezérlést kombinálja. A kiszolgáló alapú tűzfalak kevésbé biztonságosak lehetnek mint az erre a célra kijelölt, eszköz-alapú tűzfalak az általános célú OS biztonsági hiányosságai miatt.

Linksys vezetéknélküli forgalomirányító beépített tűzfallal.

A legtöbb otthoni integrált forgalomirányító rendelkezik alapvető tűzfal-szolgáltatásokkal: csomag-, alkalmazás- és web hely szűrés. A nagyteljesítményű forgalomirányítók speciális operációs rendszerrel (pl.: Cisco Internetwork Operating System - IOS) szintén biztosítanak konfigurálható tűzfal szolgáltatásokat.

Személyes tűzfal

Az ügyfél oldalon helyezkednek el, és leggyakrabban SPI-alapú szűrést végeznek. A felhasználó engedélyére van szükség bizonyos alkalmazások kapcsolódásához, vagy egy listában előre tárolhatók a nem engedélyezett alkalmazások. A személyi tűzfalakat leggyakrabban akkor használják, amikor a munkaállomás közvetlenül csatlakozik a szolgáltató (ISP) modemjéhez. A hibás konfiguráció akadályozhatja az Internet forgalmat. Egyidejűleg ne használjunk több személyi tűzfalat, mert akadályozhatják egymás munkáját.

8.4.2 A tűzfal használata

A tűzfalaknak, mint határkészüléknek, a belső hálózat (intranet) és az Internet közé helyezésével minden kifelé és befelé irányuló Internet forgalom megfigyelhető és ellenőrizhető. Ez egyértelmű védelmi vonalat létesít a belső és külső hálózat között. Mindemellett néhány külső ügyfélnek szüksége lehet a belső erőforrások használatára. Ennek biztosítására lehet kiépíteni a demilitarizált zónát (DMZ).

A demilitarizált zóna kifejezés a hadseregtől lett kölcsönözve, ahol a DMZ két haderő között kijelölt olyan terület, ahol tilos katonai tevékenység folytatása. A számítógépes hálózatok világában a DMZ a hálózat egy olyan területére vonatkozik, mely mind a belső, mind a külső felhasználók számára hozzáférhető. Biztonságosabb, mint a külső hálózat, de nem olyan biztonságos, mint a belső hálózat. A belső hálózatot, a DMZ-t és a külső hálózatot egy vagy több tűzfallal különítik el. A nyilvános hozzáférésű webkiszolgálókat gyakran a DMZ-ben helyezik el.

Egytűzfalas konfiguráció

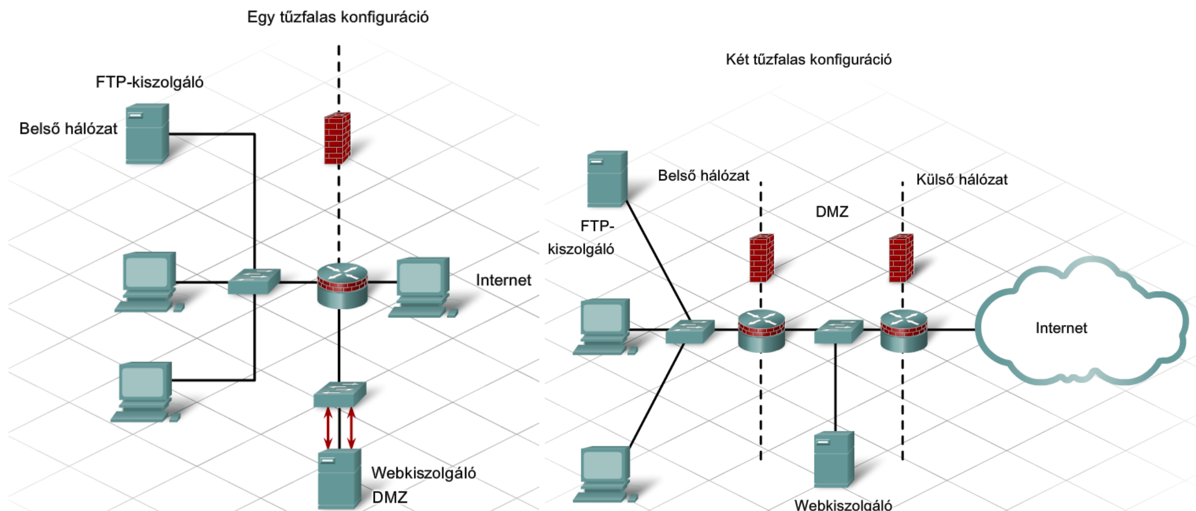
Az egyedüli tűzfal három területtel rendelkezik, egy-egy területtel a külső hálózat, a belső hálózat, és a DMZ számára. Minden külső hálózatból származó forgalom a tűzfalhoz kerül elküldésre. A tűzfallal szembeni elvárás az is, hogy ellenőrizze a forgalmat és határozza meg, hogy mely forgalmat kell a DMZ-be, melyet kell a belső hálózatba továbbítani és melyet kell végképp elutasítani.

Kéttűzfalas konfiguráció

A két tűzfalas konfigurációnál egy belső és egy külső tűzfal található a kettőjük között elhelyezkedő DMZ-vel együtt. A külső tűzfal kevésbé korlátozó és megengedi, hogy az Internet felhasználók hozzáférjenek a DMZ-ben levő szolgáltatásokhoz valamint megengedi, hogy bármely belső felhasználó által kért forgalom áthaladjon rajta. A belső tűzfal jóval korlátozóbb és védi a belső hálózatot a jogosulatlan hozzáféréstől.

Az egytűzfalas konfiguráció a kisebb, kevésbé terhelt hálózatokhoz megfelelő. Mindemellett az egytűzfalas konfiguráció egyetlen meghibásodási ponttal rendelkezik és túlterhelhető. A kéttűzfalas

konfiguráció inkább az olyan nagyobb, összetettebb hálózatok számára alkalmas melyek jóval nagyobb forgalmat bonyolítanak le.



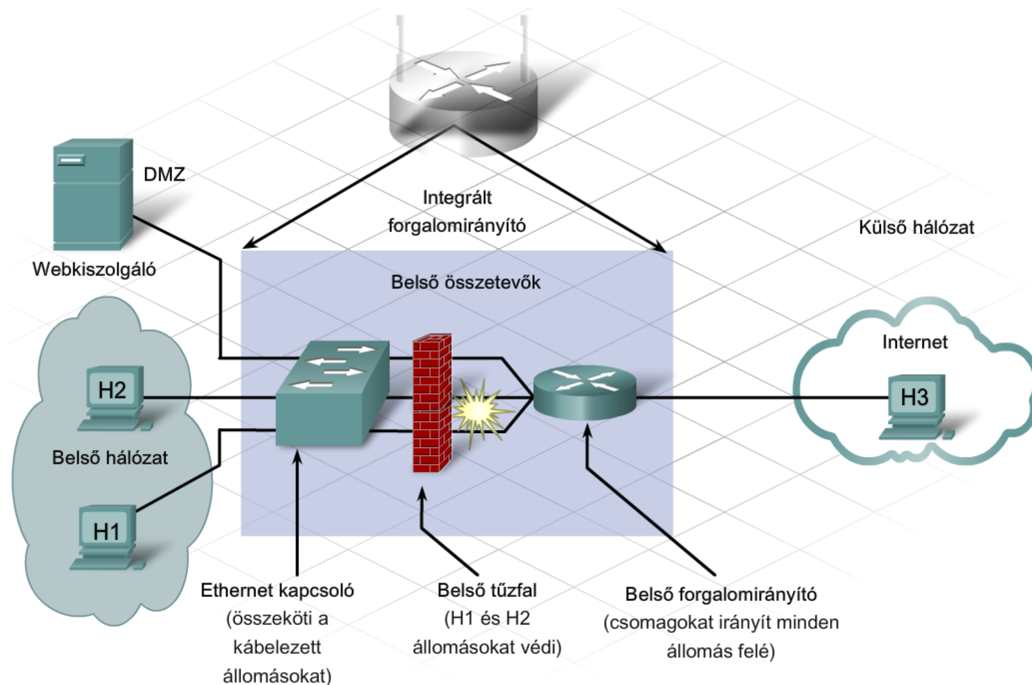
Sok otthoni eszköz, mint például egy integrált forgalomirányító, gyakran többfunkciós tűzfalszoftvert tartalmaz. Az ilyen tűzfal jellemzően hálózati címfordítás (Network Address Translation, NAT), állapot alapú csomagvizsgálat (Stateful Packet Inspection, SPI), és IP, alkalmazás és webhely szűrő képességgel rendelkezik. Ezen kívül támogatja a DMZ lehetőségét is.

Az integrált forgalomirányítóval egy olyan egyszerű DMZ állítható be, amely megengedi, hogy egy belső kiszolgáló a külső állomások számára hozzáférhető legyen. Ennek megvalósítása érdekében a kiszolgálónak statikus IP-címre van szüksége, melyet a DMZ konfigurációban meg kell határozni. Az integrált forgalomirányító elkülöníti a meghatározott cél IP-című forgalmat. Ez a forgalom csak ahhoz a kapcsolóporthoz lesz továbbítva, amelyhez a kiszolgáló kapcsolódik. Az összes többi állomást így még inkább védi a tűzfal.

Amikor a DMZ a legegyszerűbb formájában áll rendelkezésre, akkor a külső állomások a kiszolgáló minden portjához hozzáférhetnek (pl.: 80 - HTTP, 21- FTP, 110 - E-mail POP3, stb.).

A port-alapú továbbítás használatával, jóval korlátozóbb DMZ állítható be. A port-alapú továbbítás esetén meg vannak határozva azok a portok melyek a kiszolgálón elérhetők. Ebben az esetben csak az adott célportokra irányuló forgalom engedélyezett, minden más forgalom tiltott.

Az integrált forgalomirányítón belüli vezeték nélküli elérési pont a belső hálózat részének tekintendő. Fontos annak megértése, hogy ha a vezeték nélküli elérési pont nem biztonságos, bárki, aki ahhoz csatlakozik a belső hálózat védett részére, a tűzfal mögé kerül. A hekkerek (hacker) így a biztonsági szolgáltatások kikerülésével juthatnak a belső hálózatba.



8.4.3 A sebezhetőség elemzése

Az állomások és a hálózat biztonságának ellenőrzésére számos elemző eszköz áll rendelkezésre. Ezek a biztonságvizsgálóként ismert eszközök segítenek azoknak a területeknek az azonosításában, ahol támadás jelentkezhet, és iránymutatást adnak a teendő óvintézkedésekre. A sebezhetőség vizsgáló eszköz szolgáltatásai gyártótól függően változhatnak, közös szolgáltatásaik közé tartoznak:

- A hálózaton rendelkezésre álló állomások számának megadása.
- Az állomások által nyújtott szolgáltatások felsorolása.
- Az állomás operációs rendszerének és verziószámának megadása.
- A használt csomagszűrők és tűzfalak megadása.

8.4.4 Bevált módszerek

Számos módszer létezik a kockázatcsökkentés elősegítésére. Néhány közülük:

- Határozzuk meg a biztonsági irányelveket.
- Fizikailag védjük a kiszolgálókat és a hálózati berendezéseket.
- Állítsuk be bejelentkezési és fájlhozzáférési engedélyeket.
- Frissítsük az OS-t és az alkalmazásokat.
- Változtassuk meg a megengedő alapbeállításokat.
- Futtassuk le a vírusirtót és a kémprogram-irtót.
- Frissítsük a vírusirtó szoftvert.
- Kapcsoljuk be a böngésző biztonsági eszközeit - előugró ablakok (pop-up) blokkolása, adathalászat szűrő, beépülő modulok ellenőrzése.
- Használjunk tűzfalat.

A hálózat biztonságának irányába tett első lépés, hogy tisztában legyünk a forgalom haladásával a hálózaton keresztül, és hogy megismerjük a különböző veszélyforrásokat és a sebezhető pontokat. A biztonsági intézkedések megvalósítása után, egy valóban biztonságos hálózat megköveteli a

folyamatos megfigyelést. A biztonsági eljárásokat és eszközöket folyamatosan felül kell vizsgálnunk, hogy lépést tudjunk tartani az egyre fejlődő fenyegetésekkel.

8.5 A fejezet összefoglalása

Ez a fejezet különböző hálózati fenyegetésekkel foglalkozik: adatlopás, személyazonosság eltulajdonítása, adatvesztés és adatváltoztatás, valamint a szolgáltatás megszakítása.

- A hekkerek olyan betörők, akik a hardvert érintő támadással, a szoftverek sebezhető pontjait vagy a hálózati felhasználók gondatlanságát kihasználva hozzáférést szereznek a hálózathoz.
- A támadások származhatnak mind belső mind külső forrásból. A biztonságot sértő események 70%-át belső támadások teszik ki.
- A megtévesztési techika (Social engineering) a technikák egy olyan csoportja melyet arra használnak, hogy rávegyék a belső felhasználókat meghatározott tevékenységek végrehajtására vagy bizalmas információk kiszolgáltatására.
- A megtévesztési technika három típusa a következő: hamis ürügy (pretext), adathalászat és telefonos adathalászat.

A megtévesztési technikán alapuló támadásokon kívül, a hálózatokra és számítógépekre leselkedő más veszélyek is vannak.

- A vírusok olyan programok, melyek ha egyszer aktíválva lettek más programok vagy állományok módosításával terjednek az állományok károsodását vagy teljes törlését előidézve.
- A féreg hasonló a vírushoz kivéve azt, hogy önállóan fut és önmaga példányainak e-mail mellékletként vagy a hálózati üzenet részeként történő elküldésével terjed.
- A Trójai ló oylan program, mely hivatalosnak tünteti fel magát. Ha egyszer futtatjuk, akkor károsíthatja a merevlemezt vagy hátsó ajtót (back door) nyit a rendszeren lehetővé téve a hekkereknek, hogy bejussanak.

Valódi hálózati biztonság a termékek és szolgáltatások kombinációját egyesítő átfogó biztonságpolitikából és a politikához való ragaszkodás iránti elkötelezettségből származik.

- A biztonságpolitikának tartalmaznia kell az azonosítási és hitelesítési politikákat, jelszóházirendeket, elfogadható használat rendjét, távoli elérés rendjeit és a váratlan események kezelésének eljárásait.
- A hálózat minden felhasználójának támogatnia és be kell tartania biztonságpolitikát annak érdekében, hogy az hatékony legyen.
- A hálózat biztosítására használt eszközök és alkalmazások a következőket foglalják magukban:
  - Szoftver kiegészítések és frissítések
  - Vírusvédelem
  - Kémprogramok elleni védelem
  - Levélszemét blokkolók



    - Előugró ablak blokkolók
    - Tűzfalak
- Tartsa naprakész állapotban a szoftveres alkalmazásokat a legutolsó biztonsági kiegészítésekkel (patch) és frissítésekkel a veszélyek megakadályozásának elősegítésére.
- A minden számítógépre telepített vírusirtó program észleli és eltávolítja az ismert vírusokat, férgeket és Trójai lovakat.
- A kémprogram-irtó szoftver azonosítja és egy szeméttároló mappába (karantén) helyezi vagy törli a levélszemetet.

A tűzfal a hálózatok közötti forgalmat ellenőrzi és segít a jogosulatlan hozzáférés megakadályozásában. A tűzfal termékek különféle technikákat használnak annak meghatározására, hogy mi számít engedélyezett és mi tiltott hálózati hozzáférésnek. * A csomagszűrés a hozzáférést az IP vagy MAC-címek alapján vezérli.

- Az Alkalmazás/webhely szűrés a hozzáférést az alkalmazás alapján vezérli.
- Az állapot-alapú csomagvizsgálat (SPI) biztosítja azt, hogy a bejövő csomagok hivatalos válaszok legyenek a belső állomástól érkező kérésekre. Az SPI képes felismerni és kiszűrni az olyan támadásokat, mint a DoS.
- A DMZ egy olyan hálózati terület, amely mind a belső, mind a külső felhasználók számára hozzáférhető.
- Ha a vezeték nélküli hozzáférési pont nem biztonságos, akkor bárki aki kapcsolódik hozzá úgy tekintendő, hogy a belső hálózat része és a tűzfallal védett területen belül tartózkodik.
- A sebezhetőség-elemző eszközök (biztonság-vizsgálók) segítik azonosítani azokat a területeket, ahol támadások jelentkezhetnek, és iránymutatást adnak a megteendő óvintézkedésekhez.

9. Hálózati hibaelhárítás

9.1 A hibaelhárítási folyamat

9.1.1 Hibaelhárítás

A hibaelhárítás a jelentkező problémák azonosításának, a helyük meghatározásának és kijavításának folyamata. A tapasztaltabb egyének a hibaelhárítás során gyakran az ösztöneikre hallgatnak. Azonban, a legvalószínűbb ok és megoldás meghatározására strukturált technikákat használhatunk.

Amikor hibaelhárítást folytatunk, gondoskodni kell a megfelelő dokumentációról. A dokumentációnak a lehető legtöbb információt kell tartalmaznia a következőkről:

- A probléma jelentkezése.
- A probléma meghatározása során megtett lépések.
- A probléma megoldásához vezető lépések és azon lépések, melyek biztosítják, hogy a probléma újból ne történjen meg.

Dokumentáljunk minden lépést a hibaelhárítás folyamán, még azokat is, melyek nem oldották meg a problémát. A dokumentáció értékes referenciává válik, ha ugyanaz a hiba vagy egy ahhoz hasonló ismét jelentkezik.

9.1.2 Információgyűjtés

Amikor egy hibát jelentenek, ellenőrizzük és határozzuk meg a hiba nagyságát. Amint a probléma létezését megerősítettük, a hibaelhárítás első lépésében információt gyűjtünk.

Hibaelhárítási információs lista

A probléma természete
- ✓ Végfelhasználói jelentések
- ✓ A probléma létezésének megerősítése

Készülék
- ✓ Gyártó
- ✓ Gyártmány / Modell
- ✓ Firmware verzió
- ✓ Operációs rendszer verziószám
- ✓ Tulajdonosi / jótállási információ

Konfiguráció és topológia
- ✓ Fizikai és logikai topológia
- ✓ Konfigurációs fájlok
- ✓ Naplóállományok

Előző hibaelhárítás
- ✓ Lépések és eredmények

Az információgyűjtés egyik kezdeti módja, hogy kikérdezzük a problémáról beszámoló egyént, csakúgy, mint a többi érintett felhasználót. A kérdés magában foglalhat: végfelhasználói tapasztalatokat, megfigyelt tüneteket, hibaüzeneteket és az eszközök, alkalmazások újonnan változtatott beállításaival kapcsolatos információkat.

Következő lépésben, információt gyűjtünk minden eszközről, mely érintve lehet. Ez a dokumentációk alapján elvégezhető. Továbbá szükséges a naplófájlokról egy másolat és egy lista, a berendezések konfigurációjában utóbb végzett változtatásokról. A berendezésen található egyéb információ magában foglalja a gyártót, az érintett eszköz megnevezését és típusát, csakúgy, mint a tulajdonost és a garancia információkat. Az eszköz firmware vagy szoftver verziója szintén fontos, mert egyes hardver-platformokkal kompatibilitási problémák lehetnek.

Hálózattal kapcsolatos információkat is gyűjthetünk hálózatfigyelő eszközök használatával. A hálózatfigyelő eszközök komplex alkalmazások, melyeket gyakran használnak nagy hálózatokban a hálózat és a hálózati eszközök állapotával kapcsolatos adatok folyamatos gyűjtésére. Ezek az eszközök kisebb hálózatok számára lehet, hogy nem érhetőek el.

Miután minden szükséges információt beszereztünk, elkezdhetjük a hibaelhárítási folyamatot.

9.1.3 Hibaelhárítási módszerek

Számos különböző strukturált hibaelhárítási technika létezik, úgymint:

- Fentről lefelé
- Alulról felfelé
- Oszd meg és uralkodj

Az összes felsorolt módszer a hálózat rétegelt modellezésén alapul. A rétegelt szemléletet tükrözi például az OSI modell, melyben a kommunikáció minden funkciója hét különálló rétegbe van szétosztva. Ezen modell használatával, a hibaelhárító személy minden réteg működését ellenőrizheti, amíg a probléma helyét és határait meg nem határozza.

A fentről lefelé módszer az alkalmazási réteget vizsgálja először, majd lefelé halad. A problémát a felhasználó és az alkalmazás szemszögéből nézi. Csak egy alkalmazás nem működik vagy egyik sem? Például: a felhasználó elér különböző weblapokat az Interneten, de az elektronikus levelezést nem? A többi állomáson is tapasztalhatóak hasonlóak?

A lentről felfelé módszer a fizikai réteggel kezdi a vizsgálatot és így halad fölfelé. A fizikai réteg a hardverrel és vezetékes kapcsolatokkal foglalkozik. Nem húzódtak ki a kábelek a csatlakozókból? Ha az eszközön vannak jelzőfények, azok égnek vagy nem?

Az oszd meg és uralkodj módszer jellemzően valamelyik középső rétegnél kezdi a vizsgálatot és lefelé vagy felfelé halad. Például: lehet, hogy a hibaelhárító személy a hálózati rétegnél kezdi az IP-cím beállítási információk ellenőrzésével.

Ezek a hibaelhárítási módszerek tökéletesek lehetnek kezdő hibaelhárító személyeknek. A tapasztaltabb egyének gyakran mellőzik ezeket a strukturált módszereket és az ösztöneikbe és tapasztalataikban bíznak. Lehet, hogy kevésbé strukturált technikát pl. próbálgatás, csere - alkalmaznak.

Hibaelhárítási módszer	Működése	Alkalmazhatósági esetei	Előnyök/Hátrányok
Fentről lefelé	Mindig az alkalmazási rétegnél kezdjük és addig haladunk lefelé, míg meg nem találjuk a hibás réteget.	Alkalmasabb egyszerűbb problémák esetén vagy akkor, amikor gyanítható, hogy alkalmazási/fel-használói vagy a felsőbb rétegek érintettek.	Ha kiderül, hogy a probléma az alsóbb rétegekhez kapcsolódik, sok időt és energiát vesztettél az alkalmazási és fentebbi rétegekben.

Hibaelhárítási módszer	Működése	Alkalmazhatósági esetei	Előnyök/Hátrányok
Oszd meg és uralkodj	A körülményektől (a (jelentett problémáktól) és tapasztalatunktól függően, valamelyik rétegnél kezdjük a hibaelhárítást és lefelé vagy felfelé haladunk az OSI modell rétegeiben.	Akkor a legmegfelelőbb, ha már tapasztalattal rendelkezünk és egyértelmű jelek utalnak a problémára.	Ez a módszer hamarabb rátalál a felelős rétegére, mint a többi módszer. Ennek a módszernek a hatékony alkalmazásához tapasztalat szükséges.

Hibaelhárítási módszerek	Működése	Alkalmazhatósági esetek	Előnyök/Hátrányok
Alulról felfelé	Mindig a fizikai réteggel kezd és addig halad, amíg meg nem találja a meghibásodott réteget.	Összetettebb eseteknél alkalmazható.	Lassú, de megbízható eljárás. Amikor a probléma az alkalmazáshoz (vagy felsőbb rétegekhez) kapcsolódik, ez a módszer hosszadalmas lehet.

Próbálgatás

A próbálgatás egyéni tapasztalatra támaszkodik, hogy meghatározza a probléma legvalószínűbb okát. A hibaelhárító személy a hálózati struktúra ismeretét és a tapasztalatát felhasználva egy megalapozott feltételezést hoz. Amint a megoldást megvalósítottuk és nem működik, a hibaelhárító személy ezt az információt felhasználva, megállapítja a hiba második legvalószínűbb okát. A folyamatot addig ismétli, míg a problémát be nem határolja, és meg nem oldja.

Amíg a próbálgatás módszere lehet rendkívül gyors is, a hibaelhárító személy képességein és tapasztalatán múlik, helytelen feltételezésekhez vezethet és az egyszerű megoldások elkerülhetik a figyelmet.

Helyettesítés

Ezen technika alkalmazása során feltételezzük, hogy a problémát egy bizonyos hardverkomponens vagy konfigurációs állomány okozza. A hibás alkatrészt vagy kódot kicseréljük egy biztosan jó eszközre vagy állományra. Bár nem feltétlenül határozzuk meg a probléma helyét, ezzel a technikával időt takaríthatunk meg és gyorsan helyreállíthatjuk a hálózat működését. Ehhez azonban a kicserélendő alkatrésznek, komponensnek és az állományokról egy biztonsági mentésnek kell elérhetőnek lenni, amit fenntartani nagyon költséges lehet.

A helyettesítéses technikára példa, amikor az internetszolgáltató kicseréli a valószínűleg meghibásodott eszközt, ahelyett, hogy egy szakembert küldene, aki elhárítaná a hibát és meghatározná a konkrét problémát. Ezt a technikát gyakran alkalmazzák még az olcsó alkatrészek esetén; mint például a hálózati kártya vagy patch kábelek cseréjét.

9.2 Hibaelhárítási vonatkozások

9.2.1 Fizikai problémák felismerése

A hálózati problémák nagy része fizikai komponensekkel vagy a fizikai réteggel van kapcsolatban.

A fizikai problémák főként a számítógépek, hálózati eszközök és az őket összekötő kábelek hardveres részével vannak kapcsolatban. A fizikai problémák nincsenek tekintettel az eszközök logikai (szoftveres) konfigurációjára.

Fizikai problémák egyaránt jelentkezhetnek vezetékes és vezeték nélküli hálózatokban. A fizikai problémák felismerésének egyik legjobb módja az érzékszerveink használata - látás, szaglás, tapintás és hallás.

Látás

A szemrevételezést használjuk olyan problémák észlelésére, mint a nem megfelelően csatlakoztatott vagy rosszul elkészített kábelek, ideértve:

- a nem csatlakoztatott kábeleket
- rossz portba csatlakoztatott kábeleket
- megszakadt kábelkapcsolatok
- sérült vezetékek és kapcsolók
- Rossz kábeltípus használata

A szemrevételezés lehetővé teszi számunkra, hogy a LED-el ellátott különböző hálózati eszközök állapotait és működését megfigyeljük.

Szaglás

A szaglás figyelmezteti a hibaelhárító személyt túlmelegedő alkatrészre. A túlmelegedett szigetelés vagy alkatrész szaga nagyon egyértelmű és komoly hiba biztos jele.

Tapintás

A hibaelhárító személy tapintással érzékelheti a túlmelegedett alkatrészeket, és felismerheti az eszközök olyan mechanikai problémáit, mint a hűtőventilátorral kapcsolatos meghibásodások. Ezek az eszközök rendszerint egy kis rezgést okoznak a részegységben, mely tapintással észlelhető. Az ilyen rezgés hiánya, vagy túlzott előfordulása jelzi, hogy a hűtőventilátor meghibásodott, vagy meg fog hibásodni.

Hallás

A hallást használhatjuk az olyan, főbb problémás észlelésére, mint az elektromos hibák, és annak érzékelésére, hogy a hűtőventillátorok és a diszkek megfelelően működnek-e. Minden eszköz jellegzetes hangot bocsát ki és általában minden, a normálistól eltérő hang valamilyen problémára utal.

9.2.2 Szoftver segédprogramok a kapcsolat hibaelhárítására

Számos segédprogram létezik, melyek segíthetnek a hálózati probléma felismerésében. Ezen segédprogramok többségét az operációs rendszerek parancssoros felületen használható parancsokkal biztosítják. A parancsok szintaxisa operációs rendszerektől függően változhat.

Néhány elérhető segédprogram:

- ipconfig - az IP beállításokat jeleníti meg
- ping - kapcsolat tesztelése más IP állomásokkal
- tracert - célhoz vezető út megjelenítése
- netstat - hálózati kapcsolatok megjelenítése
- nslookup - Egy céltartományról kér információt közvetlenül a név szervertől

9.2.3 Hibaelhárítás az Ipconfig használatával

Ipconfig

Az ipconfig parancsot egy állomás aktuális IP-beállításainak megtekintésére használjuk. A parancs parancssori futtatására megjelennek az alapvető beállítási információk: IP-cím, alhálózati maszk és alapértelmezett átjáró.

Ipconfig /all

Az ipconfig /all parancs további információkat jelenít meg, mint például MAC-cím, az alapértelmezett átjáró és a DNS kiszolgálók IP címe. Ez a parancs azt is jelzi, ha a DHCP engedélyezett, a DHCP kiszolgáló címét és a kapott IP címek érvényességének idejével kapcsolatos információkat.

Hogyan segítheti a hibaelhárítási folyamatot ez a segédprogram? Helyes IP-konfiguráció nélkül, egy állomás nem tud részt venni a hálózati kommunikációban. Ha az állomás nem tudja a DNS kiszolgáló helyét, nem tudja a neveket IP-címekre lefordítani.

Ipconfig /release és ipconfig /renew

Ha az IP információkat automatikusan kapjuk, az ipconfig /release parancs felszabadítja a DHPC címkötéseket. Az ipconfig /renew parancs a DHCP kiszolgálótól új konfigurációs információkat kér. Az állomás birtokolhat hibás vagy lejárt IP-konfigurációs információkat és lehet, hogy csak ezen információk egyszerű megújítási folyamata szükséges a kapcsolat helyreállításához.

Ha az IP konfiguráció felszabadítása után az állomás nem képes friss információkat szerezni a DHCP szervertől, lehet, hogy nincs hálózati kapcsolat. Ellenőrizzük, hogy a hálózati csatolónak világít-e a kapcsolatjelző világítása, jelezve, hogy létezik a hálózathoz fizikai kapcsolódás. Ha ez nem oldja meg a problémát, lehet, hogy a DHCP kiszolgálóval van a probléma vagy a DHCP kiszolgálóhoz vezető hálózati kapcsolattal.



9.2.4 Hibaelhárítás a Ping használatával

Ha a helyi állomás IP-konfigurációja helyesnek bizonyult, a következő lépésben a ping használatával teszteljük a hálózati kapcsolódást. A ping parancsot a célállomás elérhetőségének tesztelésére használjuk. A ping parancs után egyaránt írhatjuk a célállomás IP címét, vagy a nevét, például:

- ping 192.168.7.5
- ping www.cisco.com

Amikor egy ping-et küldünk egy IP-címre, egy visszhangkérésként ismert csomagot küldünk a megadott IP-címre a hálózaton keresztül. Ha a célállomás megkapja a visszhangkérést, egy visszhangválaszként ismert csomaggal válaszol. Ha a forrás megkapja a visszhangválaszt a kapcsolat meg van erősítve.

Ha a ping-et egy névnek küldik el, úgy, mint www.cisco.com, a csomag először a DNS kiszolgálóhoz lesz elküldve, hogy az a nevet IP címre oldja fel. Miután megkapta az IP-címet, a visszhangkérést továbbítja az IP-cím felé és a folyamat tovább folytatódik. Ha az IP-cím pingelése sikeres volt, de a név pingelése nem, a probléma valószínűleg a DNS-sel van.

Ha a ping mind a név, mind pedig az IP-cím esetén sikeres, de a felhasználó még mindig nem tudja az alkalmazást elérni, akkor a probléma valószínűleg a célállomás alkalmazásában van. Például, lehet, hogy a kért szolgáltatás nem fut.

Ha a ping sem sikeres, akkor valószínűleg a célhoz vezető út hálózati összeköttetésében van a hiba. Ha ez történik, általános gyakorlat, hogy az alapértelmezett átjárót pingeljük. Ha az alapértelmezett átjáró pingelése sikerrel járt, a probléma nem helyi eredetű. Ha az alapértelmezett átjáró pingelése sikertelen, a probléma a helyi hálózatban van.

Az alap ping parancs négy visszhangkérést küld, és egyenként várja a válaszokat. Azonban ez változtatható a nagyobb hasznosság érdekében. Az ábrán látható listán vannak az opciók, a további elérhető lehetőségekről.

9.2.5 Hibaelhárítás a Tracert használatával

A ping segédprogram a végpontok közötti kapcsolat tesztelésére szolgál. Azonban, ha egy probléma fennáll és az eszköz nem tudja pingelni a célt, a ping parancs nem jelzi, hogy a kapcsolat valójában hol szakadt meg. Ennek kiderítéséhez egy másik segédprogramot, a tracert használjuk.

A tracert segédprogram annak az útvonalnak a hálózati kapcsolatairól biztosít információkat, amelyen a csomag a cél felé halad, és minden forgalomirányítóról (ugrásról), amely az úton van. A tracert továbbá jelzi, hogy mennyi ideig tartott, hogy egy csomag eljusson a forrástól minden egyes ugráshoz és vissza (RTT: Round Trip Time - Oda-vissza jelterjedési idő). A tracert segíthet annak azonosításában, hogy a csomag hol veszhetett el vagy késhetett a hálózatban található torlódások és lelassulások következtében.

Az alap tracert segédprogram csak 30 ugrást engedélyez a forrás és a céleszköz között, mielőtt a célt elérhetetlennek nyilvánítaná. Ez a szám a -h paraméterrel szabályozható. Az ábrán látható Options alatti egyéb lehetőségek is elérhetők.

9.2.6 Hibaelhárítás a Netstat használatával

Néha szükséges tudni, hogy mely aktív TCP kapcsolatok vannak nyitva és melyek futnak egy hálózatba kötött állomáson. A netstat egy fontos hálózati segédprogram, mely ezen kapcsolatok ellenőrzésére használható. A netstat kilistázza a használt protokollokat, a helyi címeket és portszámokat, az idegen címeket és port számokat és a kapcsolatok állapotát.

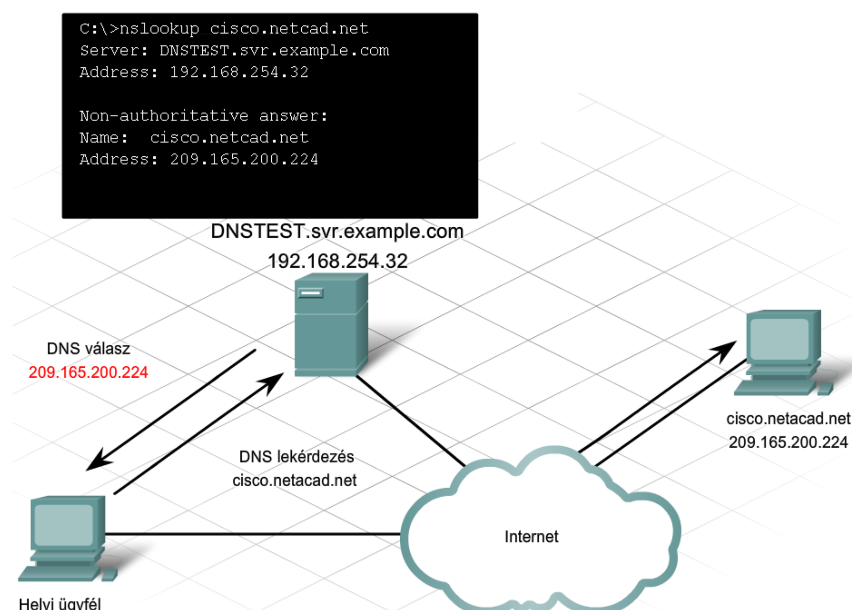
A rejtélyes TCP kapcsolatok komoly biztonsági fenyegetettséget okozhatnak. Ez azért van, mert jelzik, hogy valami vagy valaki csatlakozott az állomáshoz. Továbbá, a szükségtelen TCP kapcsolatok értékes rendszererőforrásokat emészthetnek fel, így lerontják az állomás teljesítményét. A netstat parancsot kell használni az állomás nyitott kapcsolatainak vizsgálatára, amikor a teljesítmény visszaesését érzékeljük.

Számos hasznos Opció érhető el a netstat parancshoz.

9.2.7 Hibaelhárítás az Nslookup használatával

Amikor a hálózaton keresztül alkalmazásokat vagy szolgáltatásokat érünk el, az egyének általában a DNS nevet használják IP-cím helyett. Amikor egy kérést küldünk egy névre, az állomásnak először kapcsolatba kell lépnie a DNS kiszolgálóval, hogy a nevet feloldja a megfelelő IP-címre. Az állomás a szállításhoz ezután az IP-t használja az információ becsomagolásához.

Az nslookup segédprogram lehetővé teszi a végfelhasználók számára, hogy információkat keressenek egy bizonyos DNS névről a DNS kiszolgálón. Amikor az nslookup parancsot használjuk, az információban a használt DNS kiszolgáló IP címét is megkapjuk, csakúgy, mint a konkrét DNS névhez rendelt IP-címet. Az nslookup hibaelhárító segédeszközt gyakran használjuk annak meghatározására, hogy a DNS kiszolgáló a vártnak megfelelően végzi-e a névfeloldást.



9.3 Gyakori problémák

9.3.1 Kapcsolódási problémák

Kapcsolódási problémák jelentkeznek vezeték nélküli, vezetékes hálózatokon és az olyan hálózatokban is, ahol mind a két hálózattípust használják. Amikor egy vezetékes vagy vezeték nélküli hálózat hibáit hárítjuk el, gyakran a legjobb megoldás, ha az oszd meg és uralkodj módszert használjuk a a probléma behatárolására, mind vezetékes, mind pedig vezeték nélküli hálózatokban. A legkönnyebb módja annak meghatározására, hogy a probléma a vezetékes vagy a vezeték nélküli hálózatban van, a következő:

1. Pingessük meg az alapértelmezett átjárót egy vezeték nélküli ügyfélről - ez igazolja, hogy a vezeték nélküli ügyfél a vártnak megfelelően kapcsolódik.
2. Pingessük meg az alapértelmezett átjárót egy vezetékes ügyfélről - ez igazolja, hogy a vezetékes ügyfél a vártnak megfelelően kapcsolódik.
3. Pingessük meg a vezetékes ügyfelet a vezeték nélküli ügyfélről - ez igazolja, hogy az integrált forgalomirányító a vártnak megfelelően működik.

Amint a problémát elkülönítettük, ki lehet javítani.

9.3.2 LED kijelzők

Függetlenül attól, hogy a meghibásodás a vezeték nélküli vagy vezetékes hálózatban van, a hibaelhárítási folyamat elején meg kell vizsgálni a LED-eket, melyek egy berendezés vagy egy kapcsolat aktivitását, ill. ezek aktuális állapotát jelzik. Az információt adó LED-ek villoghatnak, színei változhatnak. A LED-ek pontos konfigurációja és jelentése gyártónként és eszközönként változik.

Általában háromféle LED-et találunk az eszközökön - tápellátás, állapot és aktivitás. Néhány eszköznél egy LED többféle információt is hordozhat, az eszköz aktuális állapotától függően. A LED-ek jelzésének pontos értelmezéséhez fontos a dokumentáció áttekintése, bár létezik néhány közös vonás.

Inaktív LED jelezhet eszköz és port-hibát vagy kábel problémát. Előfordulhat, hogy az eszköz hardverhiba miatt nem működik. Maga a port is hibássá válhat a hardver vagy rosszul konfigurált szoftver miatt. Tekintet nélkül arra, hogy vezetékes vagy vezeték nélküli hálózatról van szó, ellenőrizze, hogy az eszköz és a port is be van-e kapcsolva és működik, mielőtt sok időt eltöltve megpróbálna más problémákat elhárítani!

Biztonsági LED

- Az aktuális biztonsági beállítások állapotát jelzi az eszközön
- A folyamatos zöld azt jelzi, hogy érvényben vannak a biztonsági beálltások

Aktivitást jelző LED

Néha kapcsolati lámpának is nevezik, normál esetben az aktivitást jelző LED egy bizonyos porthoz tartozik. Normál körülmények között, a villogás azt jelzi, hogy forgalom áramlik a porton. Néhány eszköznél a villogás gyakorisága jelzi a port működési sebességét.

Tépellátás LED

- Általában folyamatosan zölden világító
- Az eszköz áramellátását jelzi
- Ha nem világít, azt jelenti, hogy áramellátási problémák vannak. Ellenőrizze a tápellátást!

9.3.3 Kapcsolódási problémák

A vezetékes állomás nem tud az integrált forgalomirányítóhoz kapcsolódni

Ha a vezetékes állomás nem tud az integrált forgalomirányítóhoz kapcsolódni, az első dolog, amit ellenőrizni kell a fizikai kapcsolat és a kábelezés. A vezetékes hálózatok központi idegrendszere a kábelezés, ami az egyik leggyakoribb probléma, ha kapcsolási hibát tapasztalunk.

Néhány dolog, amire a kábelezésnél figyelni kell:

1. Legyen biztos benne, hogy a megfelelő kábeltípust használja! Kétféle UTP kábellel találkozunk gyakran a hálózatokban: egyenes- és keresztkötésű kábel. A rossz kábelhasználat megakadályozhatja a kapcsolódást.
2. A hálózatoknál az egyik fő probléma, amivel találkozhatunk, a nem megfelelően lezárt kábel. Ahhoz, hogy elkerüljük ezt, a kábeleket a szabványok szerint kell végződtetni.
   - A kábeleket a 568A vagy 568B szabványok szerint végződtesse!
   - A végződtetés során kerülje a vezetékek túlságos szétcsavarását!
   - A csatlakozókat krimpelje rá a szigetelésre!
3. A különböző kábeltípusok jellemzői alapján, létezik egy maximum kábelhossz. Ezen hosszúságok túllépése komoly negatív hatással lehet a hálózat teljesítményére.
4. Kapcsolódási probléma esetén ellenőrizze, hogy a hálózati eszközök megfelelő portjait használja!
5. Védje a kábeleket és a csatlakozókat a fizikai sérüléstől! Ügyeljen a kábelekre, hogy megakadályozza a feszülést a csatlakozóknál, és a kábelt olyan helyen vezesse végig, ahol nincsenek útban!

9.3.4 Rádiófrekvenciás problémák elhárítása egy WLAN-ban

Ha a vezeték nélküli kliens nem tud kapcsolódni az AP-hoz, az lehet, hogy vezeték nélküli kapcsolódási probléma miatt van. A vezeték nélküli kommunikációhoz az adatszállítást a rádiófrekvenciás (RF) jelek biztosítják. A rádiófrekvencia használata során, sok tényező befolyásolhatja az állomásokhoz való kapcsolódási képességünket.

1. Nem minden vezeték nélküli szabvány kompatibilis. A 802.11a (5 GHz-es sáv) nem kompatibilis a 802.11b/g/n szabványokkal (2.4 GHz-es sáv). A 2.4 GHz-es sávon belül minden szabvány más technológiát használ. Speciális konfiguráció nélkül, egy készülék, ami illeszkedik, az egyik szabványhoz lehet, hogy nem fog működni egy másik szabványhoz illeszkedő készülékkel.
2. Minden vezeték nélküli párbeszédnek különálló, átlapolás nélküli csatornán kell történnie. Néhány AP konfigurálható úgy, hogy kiválassza a legkevésbé zsúfolt vagy legnagyobb áteresztő-képességgel rendelkező csatornát. Bár az automatikus beállítások is működnek, az AP kézi csatorna-beállítása hatékonyabb irányítást biztosít és néhány környezetben szükségessé válhat.

3. Az RF jel erőssége a távolsággal csökken. Ha a jelerősség túlságosan kicsi, az eszközök képtelenek megbízhatóan kapcsolódni és adatokat mozgatni. A jel lehet, hogy megszakad. A hálózati csatoló segédprogramját használhatjuk a jelerősség és a kapcsolat minőségének megjelenítésére.
4. Az RF jelek hajlamosak külső forrásokkal interferálni, például más, azonos frekvencián működő eszközökkel. Ezek felderítésére terepfelmérést érdemes végezni.
5. Az AP-k megosztják az eszközök között a rendelkezésre álló sávszélességet. Ahogy több eszköz kapcsolódik az AP-hez, az egyes eszközökhöz tartozó sávszélesség lecsökken, hálózati teljesítmény-problémákat okozva. Erre a megoldás, hogy csökkentjük az egy csatornát használó vezeték nélküli kliensek számát.

9.3.5 Hibaelhárítás a WLAN társításban és hitelesítésben

Ha a vezeték nélküli kliens nem tud kapcsolódni az AP-hez, az lehet, hogy vezeték nélküli kapcsolódási probléma miatt van. A vezeték nélküli kommunikációhoz az adatszállítást a rádiófrekvenciás (RF) jelek biztosítják. A rádiófrekvencia használata során, sok tényező befolyásolhatja az állomásokhoz való kapcsolódási képességünket.

1. Nem minden vezeték nélküli szabvány kompatibilis. A 802.11a (5 GHz-es sáv) nem kompatibilis a 802.11b/g/n szabványokkal (2.4 GHz-es sáv). A 2.4 GHz-es sávon belül minden szabvány más technológiát használ. Speciális konfiguráció nélkül, egy készülék, ami illeszkedik, az egyik szabványhoz lehet, hogy nem fog működni egy másik szabványhoz illeszkedő készülékkel.
2. Minden vezeték nélküli párbeszédnek különálló, átlapolás nélküli csatornán kell történnie. Néhány AP konfigurálható úgy, hogy kiválassza a legkevésbé zsúfolt vagy legnagyobb áteresztő-képességgel rendelkező csatornát. Bár az automatikus beállítások is működnek, az AP kézi csatorna-beállítása hatékonyabb irányítást biztosít és néhány környezetben szükségessé válhat.
3. Az RF jel erőssége a távolsággal csökken. Ha a jelerősség túlságosan kicsi, az eszközök képtelenek megbízhatóan kapcsolódni és adatokat mozgatni. A jel lehet, hogy megszakad. A hálózati csatoló segédprogramját használhatjuk a jelerősség és a kapcsolat minőségének megjelenítésére.
4. Az RF jelek hajlamosak külső forrásokkal interferálni, például más, azonos frekvencián működő eszközökkel. Ezek felderítésére terepfelmérést érdemes végezni.
5. Az AP-k megosztják az eszközök között a rendelkezésre álló sávszélességet. Ahogy több eszköz kapcsolódik az AP-hez, az egyes eszközökhöz tartozó sávszélesség lecsökken, hálózati teljesítmény-problémákat okozva. Erre a megoldás, hogy csökkentjük az egy csatornát használó vezeték nélküli kliensek számát.

9.3.6 DHCP problémák

Ha a fizikai kapcsolat a vezetékes vagy vezeték nélküli állomásokhoz a vártnak megfelelően kiépül, akkor ellenőrizze a kliens IP beállításait!

Az IP beállítások fő hatással lehetnek az állomás hálózathoz kapcsolódási képességére. Egy integrált forgalomirányító - például a Linksys vezeték nélküli forgalomirányító - DHCP kiszolgálóként működik a vezetékes és vezeték nélküli kliensek számára, és olyan IP beállításokat biztosít, mint az IP cím, alhálózati maszk, alapértelmezett átjáró, és esetleg még a DNS kiszolgálók IP címeit is. A DHCP

kiszolgáló az IP címet a kliens MAC-címéhez köti, és a kliens táblában tárolja az információt. Az otthoni Linksys vezeték nélküli forgalomirányítónál ezt a táblát megvizsgálhatjuk a grafikus felület Állapot | Helyi hálózat oldalán.

A kliens tábla-információnak meg kell egyeznie a helyi állomás információkkal, amit lekérhetünk az ipconfig /all paranccsal. Ráadásul a kliens IP címének egy hálózatban kell lennie a Linksys LAN interfészével. Az alapértelmezett átjárónak a Linksys LAN interfészét kell beállítani. Ha a kliens információ nem egyezik meg a kliens táblában találhatóval, akkor a címet vissza kell adni, az ipconfig /release paranccsal, majd megújítani egy új kötéshez az ipconfig /renew utasítással.

Ha a vezetékes és a vezeték nélküli állomások is kapnak IP címet, csatlakozni tudnak a Linksys eszközhöz, de egymást nem tudják pingelni, akkor a probléma nagy valószínűséggel a Linksys eszközben van. Ellenőrizze a konfigurációkat a Linksys eszközön, hogy meggyőződjön arról, hogy nincs biztonsági korlátozás, ami a problémát okozná!

9.3.7 ISR és ISP kapcsolat hibaelhárítása

Ha a vezetékes vagy vezeték nélküli hálózaton az állomás kapcsolódni tud az integrált forgalomirányítóhoz vagy más helyi hálózati állomásokhoz, de nem tud az Internethez, akkor a probléma az integrált forgalomirányító és az ISP közötti kapcsolatban lehet.
Sok mód van az integrált forgalomirányító és az ISP közötti kapcsolat ellenőrzésére. Felhasználva a grafikus felhasználói felületet, az egyik módja a csatlakozás ellenőrzésének, hogy megvizsgáljuk a forgalomirányító állapotát bemutató oldalt. Ennek mutatnia kell az ISP-től kapott IP címet, és jeleznie, hogy a kapcsolat felépült.

Ha az oldal nem mutat kapcsolatot, az integrált forgalomirányító lehet, hogy nem csatlakozott. Ellenőrizzen minden fizikai kapcsolatot és a LED-et. Ha a DSL vagy Kábel modem külön eszköz, akkor ellenőrizze le azok csatlakozásait és kijelzőit is. Ha az ISP felhasználó nevet vagy jelszót igényel, akkor ellenőrizze, hogy ezek beállítása megegyezik az ISP által adott névvel és jelszóval. A grafikus felületet használva, a jelszó beállítások általában a Beállítások konfigurációja oldalon találhatók. Ezt követően, az állapot oldalon a Csatlakozás, vagy az IP cím megújítása gombra kattintva próbálja meg újra felépíteni a kapcsolatot. Ha az integrált forgalomirányító még mindig nem csatlakozik, akkor lépjen kapcsolatba az ISP-vel, hogy lássa, ha a hiba az ő oldalukon van!

Ha az állapot oldal azt mutatja, hogy a kapcsolat működik, de ha egy Internetes oldal felé a ping sikertelen, akkor lehet, hogy az adott oldal nem megy. Próbáljon meg egy másik oldalt pingelni, hogy lássa, sikeres-e. Ha nem, akkor ellenőrizze az engedélyezett biztonsági intézkedéseket, amik esetleg a problémát okozhatják, például a portszűrést!

9.4 Hibaelhárítás és ügyfélszolgálat

9.4.1 Dokumentáció

A hálózati dokumentáció fontos része a hibaelhárítási folyamatnak. A hálózati dokumentációnak tartalmaznia kell egy normál vagy viszonyítási ponthoz képesti hálózati teljesítmény eredményt, ami alapján a potenciális problémák megítélhetőek.

A teljesítményviszonyítási pont tartalmazza az elvárt, normális forgalomtípusokat éppúgy, mint a kiszolgálókhoz és eszközökhöz irányuló és a felőlük érkező forgalom nagyságát. A viszonyítási pontot a hálózat telepítése után kell dokumentálni, amikor optimálisan működik. Miután bármilyen nagyobb változtatást végzünk a hálózaton, a teljesítményi viszonyítási pontot újra meg kell állapítani.

Ezen felül, az olyan dokumentációk, mint a topológia rajza, a hálózat sematikus ábrája és a címzési sémák, értékes információt biztosítanak, amikor a hibaelhárító megpróbálja megérteni a hálózat fizikai elrendezését és az információ logikai áramlását.

Amikor hibaelhárítást végzünk, a hibaelhárítási folyamat alatt a dokumentációt karban kell tartani. Ez a dokumentáció értékes referencia lehet és használható lehet későbbi problémák megjelenésénél. Egy jó hibaelhárítási dokumentációnak a következőket kell tartalmaznia:

- Kezdeti probléma
- A probléma behatárolásának érdekében tett lépések
- A lépesések eredményei, a sikereseké és a sikerteleneké egyaránt
- A probléma meghatározott végső oka
- A probléma végső megoldása
- Megelőző intézkedések

9.4.2 Külső segítségforrás használata

Ha a hibaelhárítás során a hibaelhárító képtelen megtalálni a problémát és annak megoldását, akkor szükség lehet külső segítség igénybevételére. A leggyakoribb információforrások a következők:

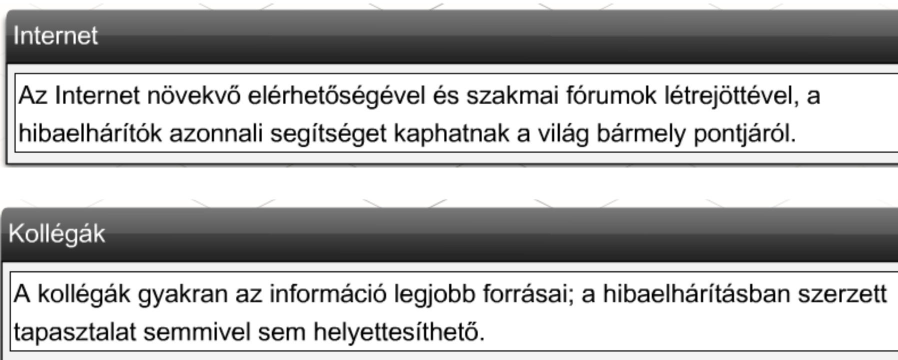
- Előző dokumentációk
- Online GYIK (Gyakran Ismételt Kérdések)
- Kollégák és más hálózati szakemberek
- Internetes fórumok

Dokumentáció

A jó dokumentáció sok időt és energiát takaríthat meg azáltal, hogy a legvalószínűbb problémára irányítja a hibaelhárító személy figyelmét. Továbbá, technikai információt nyújthat a probléma behatárolásához, igazolásához és kijavításához. Számos hálózati eszközhöz biztosított dokumentáció azonban csak a legalapvetőbb hibák elhárításához biztosít elegendő információt.

Gyakori kérdések

A legtöbb gyártó web oldalán Gyakran Ismételt Kérdések (GYIK) alatt megtalálhatók a termékeikkel vagy technológiáikkal kapcsolatos kérdések és válaszok. Többnyire az ügyfelek korábban felmerült kérdésein alapulnak, friss információforrás, érdemes olvasgatni.



9.4.3 Ügyfélszolgálat használata

Az ügyfélszolgálat az első állomás a végfelhasználók segítségnyújtásához. Az ügyfélszolgálat személyek egy csoportja a szükséges tudással és segédeszközökkel, akik segítenek megállapítani és kijavítani a problémákat. Segítséget biztosítanak a végfelhasználóknak, hogy megállapítsák a probléma létezését, természetét és megoldását.

Sok vállalat és ISP ügyfélszolgálatot hoz létre, hogy ezzel nyújtsanak segítséget az ügyfeleik hálózati problémáiban. A legtöbb nagy IT vállalat ügyfélszolgálatot üzemeltet a saját termékükhöz vagy technológiájukhoz. Például, a Cisco Systems ügyfélszolgálati segítséget kínál a Cisco eszközök hálózatba integrálásához, vagy a telepítés utána problémákhoz.

Sokféle módon léphetünk kapcsolatba az ügyfélszolgálattal: elektronikus levélben, élő beszélgetésben és telefonon. Amíg az elektronikus levél megfelelő a nem sürgős problémák esetében, hálózati vészhelyzetek esetén jobb a telefon és az élő beszélgetés. Ez különösen fontos olyan szervezeteknél, mint a bankok, ahol rövid leállás is sok pénzbe kerülhet.

Ha szükséges az ügyfélszolgálat átveheti a helyi állomás irányítását távoli hozzáférést biztosító programon keresztül. Ez lehetővé teszi az ügyfélszolgálati technikusoknak, hogy diagnosztikai programokat futtassanak, és kapcsolatba lépjenek az állomással és a hálózattal, anélkül, hogy fizikailag a munka helyszínére utaznának. Ez nagyban lecsökkenti a várakozási időt a probléma megoldására, és lehetővé teszi az ügyfélszolgálatnak, hogy több felhasználót támogassanak.

Végfelhasználóként fontos, hogy annyi információt bocsássunk az ügyfélszolgálatos részére, amennyit csak lehet. Az ügyfélszolgálat információt fog kérni minden szolgáltatásról, vagy az érvényben lévő támogatási tervről, amiben az adott eszközt specifikáló részletek vannak. Ez magában foglalja a gyártó, modell és sorozatszám mellett a firmware verziót vagy az eszközön futó operációs rendszert. Lehet, hogy a hibásan működő eszköz és IP- és MAC-címét is igényelni fogják. Az ügyfélszolgálat a problémát specifikáló információt fog igényelni, ideértve:

- A mutatott tünetek
- Ki fedezte fel a problémát
- Mikor jelent meg a probléma
- A probléma azonosítása érdekében tett lépések
- A megtett lépések eredményei

Ha ez egy második hívás (az első, az ügyfélszolgálattal való kapcsolat felvétele után, a kapcsolat megerősítésére szolgáló telefonhívás), akkor legyen készen megadni az előző hívás dátumát és idejét,



a jegyszámot, és a szakértő nevét! Legyen az érintett eszköznél, és legyen készen, hogy az ügyfélszolgálat személyzetének hozzáférést biztosítson a berendezéshez, ha igénylik!

Az ügyfélszolgálat általában a tapasztalati és a tudás szint alapján szerveződik. Ha az első szintű ügyfélszolgálati személyzet nem tudja megoldani a problémát, akkor magasabb szintűek elé terjesztik. Felsőbb szintű munkatársak általában jobban informáltak és olyan erőforrásokhoz és segédeszközökhöz van hozzáférésük, amikhez az első szintű ügyfélszolgálatnak nincs.

Rögzítsen minden információt az ügyfélszolgálattal folytatott párbeszéd során, mint például:

- A hívás ideje/dátuma
- A szakértő neve/azonosítója
- A jelentett probléma
- A megtett lépések folyamata
- Megoldás/kiterjesztés
- Következő lépés (azt követő)

Az ügyfélszolgálattal való együtt működéssel a legtöbb probléma gyorsan és könnyen megoldható. Amikor megoldódott, légy biztos, hogy minden dokumentáció frissítve lett, hogy a jövőben hivatkozni lehessen rá!

9.5 A fejezet összefoglalása

Ez a fejezet problémák felismerésének, helyük meghatározásának és megoldásának folyamatával foglalkozik.

- A hibaelhárítási folyamat fontos első lépése az információgyűjtés és annak ellenőrzése, hogy a probléma létezik
- Hibaelhárításkor sokféle strukturált hibaelhárítási technikát használhatunk, például: fentről lefelé, lentről felfelé, oszd meg és uralkodj.
- Kevésbé strukturált technika a próbálgatás és a helyettesítés
- A hibaelhárítási eseteknél a tapasztalt hibaelhárítók egyre inkább a tapasztalatukban és a kevésbé strukturált technikákban bíznak.

Sok segédeszköz van a hibaelhárítási folyamat segítésére.

- A fizikai problémák főként az eszközök hardverét valamint a kábeles kapcsolatokat érintik.
- A fizikai problémákat gyakran az érzékeinkkel észleljük.
- Számos segédprogram létezik, melyek segíthetnek a hálózati problémák azonosításában.
- A hibaelhárításnál leggyakrabban használt segédprogramok: ipconfig, ping, tracert, nslookup, netstat.

A vezetékes és vezeték nélküli hálózatok hibaelhárításakor sok dolgot kell ellenőrizni.

- A LED-ek az eszköz egy részének vagy a kapcsolat egy pillanatnyi állapotának vagy aktivitásának jelzésére szolgálnak.



- A vezetékes eszközöknél ellenőrizze a fizikai kapcsolódást és a kábelezési problémákat, beleértve a helytelen kábeltípust, a rossz lezárást, a fizikai károsodást, a portcsatlakoztatásokat!
- A vezeték nélküli ügyfeleknél a következő kapcsolódási problémákat kell vizsgálni: A/B/G/N kompatibilitás, csatornák közötti átfedés, jelerősség, interferencia. Az SSID-t, hitelesítést és titkosítást is ellenőrizze!
- Mind a vezetékes mind a vezeték nélküli ügyfelek esetén, ellenőrizze az ügyfél IP beállításait, köztük az IP-címet, az alhálózati maszkot, az alapértelmezett átjárót és a DNS információkat!
- Ellenőrizze a kapcsolatot az ISR és az ISP között a forgalomirányító állapot-oldalának vizsgálatával, hogy megbizonyosodjon arról, hogy az ISP-től kapott IP-cím, és a kapcsolat is jó!

Hibaelhárítás esetén számos segítségforrás van.

- Dokumentációk, mint például topológiai térképek, hálózati ábrák, címzési táblázatok segítik a hibaelhárítási tevékenységet.
- A hibaelhárítás segítésére külső erőforrások is elérhetőek: előzetes dokumentációk, online GYIK, kollégák, más hálózati szakemberek, Internetes fórumok.
- Az ügyféltámogatás, a személyek egy olyan csoportja a szükséges tudással és segédeszközökkel, akik segítenek megállapítani és kijavítani a gyakori problémákat.
- A probléma megoldásának elősegítésére gyakran első, másod és harmad szintű ügyféltámogatás áll rendelkezésre egyre kiterjedtebb helyi eljárásokkal, hogy segítsenek a problémák megoldásában.
- Fontos, hogy a hibaelhárítási folyamat összes lépését dokumentáljuk, beleértve az ügyféltámogatással folytatott párbeszédeket is.

Tartalom